George-Marius Șinca

GUVERNANȚA SECURITĂȚII NAȚIONALE

MANAGEMENTUL SECURITĂȚII SPAȚIULUI VIRTUAL ÎNTRE REALISM ȘI SUPRANAȚIONALISM



Presa Universitară Clujeană

GEORGE-MARIUS ȘINCA

GUVERNANȚA SECURITĂȚII NAȚIONALE

Managementul securității spațiului virtual între realism și supranaționalism

Presa Universitară Clujeană

2024

Referenți științifici:
Prof. univ. dr **Adrian-Liviu IVAN**
CȘ. I dr. Lucian **NASTASĂ-KOVACS**
Acad. prof. univ. dr. **Dorel BANABIC**

ISBN 978-606-37-2251-6

Universitatea Babeş-Bolyai
Presa Universitară Clujeană
Director: Codruţa Săcelean
Str. Hasdeu nr. 51
400371 Cluj-Napoca, România
Tel./fax: (+40)-264-597.401
E-mail: editura@ubbcluj.ro
http://www.editura.ubbcluj.ro/

Cuprins

ARGUMENT 8

MOTIVAȚIA ALEGERII TEMEI DE CERCETARE 28

CUVINTE CHEIE 31

GLOSAR DE ABREVIERI ȘI ACRONIME 35

CAPITOLUL I.INTRODUCERE 41

CAPITOLUL II. MANAGEMENTUL INFORMAȚIILOR ELECTRONICE VEHICULATE ÎN MEDIUL VIRTUAL 58

II.1. Organizația sursă generatoare de securitate a informației 62

II.1.1. Analiza organizației 65

II.2. Informația în organizație 71

II.2.1. Forma și conținutul informației utile 73

II.2.2. Valoarea informației 77

II.2.3. Moduri și canalele de comunicare a informației 79

II.2.4. Protejarea informației vehiculate în mediul virtual 82

II.2.5. Managementul informației electronice în organizație 86

II.3. Condiția informației vitale 88

II.3.1. Clasificarea informației 90

II.3.2. Cadru normativ și legislativ românesc privind prelucrarea datelor și informațiilor 95

II.3.3. Criterii generale ale clasificării informațiilor în organizație 98
II.3.4. Sistemul decizional bazat pe sisteme informaționale. 99
II.3.5. Surse generatoare de insecuritate informațională 103
II.4. Managementul riscului în organizație 106
II.4.1. Elita, actorul de securitate și decidentul 107
II.4.2. Riscul cibernetic - Cadru de analiză 112
II.4.3. Modelul cibernetic al managementului riscului 117
II.4.4. Minimizarea Riscului. 119
II.4.5. Predicție și previziune – Riscurile securității cibernetice în 2019. 121
II.4.6. Capacități necesare unui management al riscului competitiv în organizațiile digitalizate 131
II.4.7. Aplicarea și implementarea politicilor de securitate asupra sistemelor informaționale în mediile virtuale. 135
II.5. Teoria schimbărilor 142
Concluzii preliminare. 146

CAPITOLUL III. GUVERNANȚA SPAȚIULUI VIRTUAL ÎN CONCEPȚIA REALISMULUI ȘI SUPRANAȚIONALISMULUI 151
III. 1. Implicațiile arealului cibernetic asupra relațiilor internaționale în viziunea teoriilor realismului. 151
III.3.1. Raportul forțelor din mediul internațional în contextul realismului 152
III.1.2. Școala de gândire realistă. 154
III.1.3. Echilibrul puterilor 158
III.1.4. Puterea cibernetică în contextul realismului contemporan 159
III.1.5. Neorealismul și distribuția puterii 165
III.1.6. Punctele tari și puncte slabe ale realismului 169
III.1.7. Realismul aplicat: securitatea cibernetică 169
III.1.8. Conceptul de anarhie în contextul securității cibernetice 176
III.1.9. Cursa înarmărilor cibernetice. 179
III.1.10. Analiza „spiralei” de (in)securitate cibernetică în context contemporan. 182

III.1.11. Teoretizarea balanței ofensiv-defensiv în sectorul cibernetic . . . 191
III.2. Supranaționalism . . . 194
III.2.1. Supranaționalism și securitate cibernetică . . . 201
III.2.2. Istoricul atacurilor cibernetice . . . 204
III.2.3. Guvernare supranațională elitistă asupra sectorului de securitate cibernetic . . . 212
III.2.4. Teoria elitelor și decidentul în actul de guvernare a spațiului cibernetic . . . 213
III.2.5. Actorul de securitate . . . 215
III.2.6. Organigrama sectoarelor securității cibernetice din spațiului cibernetic . . . 216
Concluzii preliminare . . . 222

CAPITOLUL IV.DIPLOMAȚIA ÎN SPAȚIULUI CIBERNETIC . . 225
VI.1. *„România Digitală"* o nouă perspectivă . . . 225
IV.2. Diplomația digitală și Diplomația cibernetică . . . 230
IV.2.1. Tehnologia *„Big Data"* și Diplomația digitală . . . 235
IV.2.2. Tehnologii de comunicare și monitorizare . . . 236
IV.2.3. Instrumentarul diplomatic digital . . . 238
IV.2.4. Rețelele diplomatice - interdependența real/virtual . . . 242
IV.2.5. Culegerea de informații și managementul cunoașterii . . . 245
IV.3. Securitate diplomatică și guvernare prin reziliență cibernetică . . . 258
IV.3.1. Evoluția rezilienței cibernetice ca efect al politicilor de securitate diplomatică . . . 258
IV.3.2. Provocările Agendei UE în contextul securității cibernetice . . . 261
IV.3.2. Programul Europa digitală, un nou orizont, o nouă abordare . . . 265
IV.3.4. Paradigma diplomației securității cibernetice . . . 268
Concluzii preliminare . . . 270

CAPITOLUL V. INFLUENȚE ALE UNEI POLITICI UNITARE EUROPENE PRIVIND SECURITATEA INFORMAȚIEI ELECTRONICE ÎN ACTUALA STARE GEOPOLITICĂ GLOBALĂ . . 276
V.1. Abordarea de politică externă a României 276
V.1.1. Contextul securității prin reziliență cibernetică 282
V.2. Problematica securității cibernetice din perspectiva organismelor internaționale şi implicarea României ca membru al acestora 289
V.2.1. Uniunea Europeană - UE. 289
V.2.2. Organizația Tratatului Atlanticului de Nord - NATO 291
V.2.3. CONSILIUL EUROPEI - CoE 297
V.2.4. Organizația pentru Securitate și Cooperare în Europa - OSCE. 300
V.3. Modele internaționale și organisme europene cu atribuții în domeniul securității cibernetice. 303
V.4. Modele și organisme naționale cu atribuții în domeniul securității cibernetice 314
V.5. Strategii de securitate cibernetică în zona UE în raport cu restul lumii 318
V.5.1. Cooperarea comunitară și internațională.. 319
Concluzii preliminare. 328

CAPITOLUL VI. STUDIU DE CAZ – CULTURA DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA 331
VI.1. Analiza statistică 334
VI.2. Identificarea necesității de conștientizare și protecție a societății contemporane în raport cu provocările cibernetice actuale și viitoare. 335
VI.3. Chestionarul de evaluare a nivelului culturii de securitate cibernetică în România 336
VI.4. Plan analitic. 339
VI.4.1. Indici descriptivi ai eșantionului 344
VI.4.2. Analiza competențelor digitale ale utilizatorilor români . 345

VI.5. Analiza culturii de securitate informațională a utilizatorilor din România . . . 356
Concluzii preliminare . . . 368

CONSIDERAȚII FINALE . . . 371
Limitări și direcții viitoare de cercetare . . . 371
Precizări referitoare la contribuțiile personale . . . 373
Concluzii . . . 376

BIBLIOGRAFIE . . . 383
Cărți (inclusiv ediții electronice) . . . 383
Articole științifice și capitole în cărți (inclusiv ediții electronice) . . . 389
Studii și publicații ale instituțiilor naționale / internaționale 398
Legislație . . . 406
Alte studii și publicații . . . 409
Surse electronice . . . 420

LISTA FIGURILOR . . . 425

ANEXE . . . 428
ANEXA NR.1. Chestionar „Cultura de securitate cibernetică în România" . . . 429
ANEXA NR.2. Macheta centralizatoare pentru chestionarul „Cultura de securitate cibernetică în România" . . . 434
ANEXA NR.3. Organigrama domeniilor guvernanței securității cibernetice . . . 436

Argument

Prin excelență, guvernarea într-un domeniu complex precum cel al securității cibernetice este un act extrem de sensibil și cu siguranță greu de împlinit, dar nu imposibil, motiv pentru care este evidentă nevoia unei abordări elitiste în vederea reconceptualizării și construirii unui sistem de management al informației, bazat în deosebi pe sistemele digitale și pe oportunitățile oferite de arealul cibernetic.

Cele mai importante argumente privind alegerea temei de cercetare sunt subliniate în cele ce urmează sub forma unor observații preliminare ale autorului, alese din actualul context de securitate cibernetică din România. Motivația alegerii temei este datorată și progresului tehnologic prin inovare și dezvoltare în știința ingineriei electrice și tehnologiei informației, urmat îndeaproape de știința securității cibernetice. În acest caz, inovația vine prin dezvoltarea unor noi arii de cercetare a gestionării și prelucrării în timp real ale marilor volume de date (trad. eng. „*Big-Data*") în domenii precum inteligența artificială și inteligența continuă[1] (trad. eng. „*Continous Intelligence*"), stocarea hibridă de date[2] (trad. En. „*Hybrid Cloud*"),

1. Salvatore Salamone, „2020 Will Be the Year of Continuous Intelligence", https://www.rtinsights.com/2020-will-be-the-year-of-continuous-intelligence/, accesat în data de 07.01.2020.
2. Nasser Abwnawar, „*A Policy-Based Management Approach to Security in Cloud Systems*", Working Paper, De Montfort University Leicester, 2020, https://www.academia.

analiza augmentată[1] care merge și mai departe, deoarece combină analiza volumelor mari de date cu algoritmii de învățare automată și procesarea limbajului natural. Aceste noi tehnologii sunt complementare unele altora, drept urmare inovarea vine în urma descoperirii unor noi posibilități de utilizare pentru acoperirea unor carențe sau pur și simplu pentru optimizarea sistemelor și proceselor. Un argument este dat de posibilitatea de utilizare a acestor tehnologii, și nu numai, în contextul perfecționării sistemului informațional pentru sporirea capacității securității naționale și cel de luare de decizii în favoarea unei bune guvernări a securității spațiului virtual românesc.

Importanța cunoașterii unui management aplicat, funcțional și competitiv al securității spațiului virtual, poate fi mai bine înțeleasă și asumată prin cunoașterea raportului beneficiilor și deserviciilor aduse unui stat membru al Uniunii Europene dat de simularea aplicată a teoriilor realismului, precum și prin analiza influențelor supranaționalismului asupra sistemului de securitate națională în România, atât în contextul geopolitic contemporan, cât și pentru obținerea unei prognoze pe termen lung, care este imperios necesară.

Privind spre noile perspective de guvernare, printr-o utilizare a sistemelor informatice, a serviciilor și soluțiilor corespondente sectorului cibernetic, precum și printr-o tendință de digitalizare a informației gestionate de instituțiile guvernamentale[2], de autoritățile publice[3] și desigur de sectorul de afaceri, identificăm o serie de situații complexe care sunt de mare interes, atât pentru sectorul privat, cât și pentru cel al securității naționale. Instrumentarul utilizat de sistemele de guvernământ existente în arealul cibernetic ajunge tot

---

edu/42910797/A_Policy-Based_Management_Approach_to_Security_in_Cloud_Systems, accesat în data de 07.01.2020.

1. SISENSE, „Augmented Analytics: the Future of Business Intelligence", https://pages.sisense.com/rs/601-OXE-081/images/Augmented%20Analytics%20The%20Future%20of%20Business%20Intelligence.pdf, accesat în data de 07.01.2020
2. ADR, https://www.adr.gov.ro/, accesat în data de 07.01.2020.
3. MCSI, SMART CITY Concept, https://www.comunicatii.gov.ro/smart-city-concept-2/, accesat în data de 07.01.2020.

mai puțin compatibil și congruent cu înțelesul nevoii de a guverna în actualul context de securitate. Calitatea managementului informației influențează considerabil capacitatea de guvernare a celor cinci planuri: maritim, terestru, aerian, virtual și într-o mică măsură cel spațial. Necesitatea guvernării planurilor tangibile - maritim, terestru, aerian și spațial - există de zeci de ani, fiind abordată corespunzător nevoilor fiecărui stat, pe când necesitatea arealului cibernetic de care *„parțial"* depindem - fără de care se pare că nu mai suntem la fel de *„productivi"*, este o nevoie relativ nouă, cu perspective și implicații în sistemele de guvernare a securității naționale cunoscute parțial. Din acest motiv identificarea, tratarea și evidențierea problematicii ridicate de utilizarea resurselor puse la dispoziție de acest nou areal este un argument în plus pentru tratarea temei de cercetare aleasă.

Argumentul fundamental al acestei lucrări este dat de nevoia identificării unei paradigme de remodelare permanentă a cadrului de guvernare a securității cibernetice. Nevoia de identificare și validare a unei astfel de teorii este datorată și caracterului dinamic, în continuă schimbare și adaptare a modelelor de guvernare ale arealului virtual la contextul de securitate global, ceea ce desigur poate reprezenta o soluție la paradigma noilor modele de guvernare atât ale securității spațiului virtual cât și ale celorlalte arealuri. Putem menționa că indiferent de sectorul care trebuie guvernat (politic, militar, societal șamd.) și indiferent de modelul de guvernanță ales, implicațiile modelului de guvernare a sectorului virtual în funcționarea celorlalte modele poate reprezenta în egală măsură un pachet de riscuri sau beneficii pentru întregul sistem de guvernare. Așadar, raportarea celorlalte domenii - din punct de vedere al impactului și interdependenței - la sistemul de guvernanță a spațiului virtual este direct proporțională cu extinderea realității în mediul cibernetic și progresul tehnologic, ceea ce nu mai reprezintă o problemă de alegere, ci una de timp și oportunitate.

În contextul de securitate european, România și-a asumat în repetate rânduri adoptarea unui sistem de guvernanță a spațiului

cibernetic, care reprezintă unul dintre pilonii esențiali ai guvernării securității naționale, alături de apărarea armată, sectorul *„diplomatic, ordine publică, activitatea de informații, contrainformații și de securitate, managementul crizelor, domeniile educației, cultură, sănătate, economic, demografie, financiar, mediu, securitatea energetică, securitatea infrastructurilor critice și a patrimoniului istoric și cultural”*[1].

Cercetarea aduce în prim plan o perspectivă asupra managementului securității informației în raport cu nevoile bunei guvernanțe în contextul securității naționale. Nivelul de securitate al țării poate fi crescut și de o cunoaștere efectivă, reală și granulară a *„bunurilor”* ce au nevoie de a fi protejate sau gestionate, drept urmare, în ceea ce privește factorul de decizie la nivel național, se observă o nevoie tot mai mare de cunoaștere și înțelegere a informației, a mediilor de propagare a acesteia, precum și a efectelor produse de acestea asupra sistemului de securitate națională. Spre exemplu, rolul dezvoltării și extinderii cadrului legal și normativ în ceea ce privește securitatea informației în România este de o importanță deosebită.

În ceea ce privește adoptarea și implementarea noilor sisteme de comunicații și tehnologia informației, precum sunt mecanismele și procesele moderne de eficientizare a fluxului informațional, pentru optimizarea raportului eficiență/cost/calitate ca element edificator, putem lua exemplul dinamica dezvoltării tehnologice a organizațiilor din sectorului privat, unde modelul general al afacerii[2] poate fi readaptat la noile oportunități sau chiar schimbat.

Desigur, fie că vorbim de sectorul public (administrație, servicii, guvernare șamd)[3] orice acțiune sau inacțiune aduce cu sine efecte

---

1. Strategia Națională de Apărare a Țării pentru perioada 2020-2024, cu nr.DSN 1/794 din 26.05.2020.
2. Modelul general al afacerii *este reprezentarea modalității prin care organizația intenționează să genereze venituri creând valoare pentru beneficiarii serviciilor care, prin utilizarea serviciilor sau consumul produselor, aduc venituri și desigur profit organizației.*
3. Conform Ioan Alexandru, *Structuri Mecanisme și Instituții Administrative*, vol.2, Ed. Sylvi, București, 1996, „Sectorul public poate furniza servicii prin ansamblurile de

financiare și pentru a putea percepe importanța acestora este normal să ne edificăm cu privire la ce reprezintă organizația din perspectiva managementului informației.

Sectorul privat este împărțit în patru mari arii[1] de interes precum:

A. **Structura organizațională** (unde este dezvoltată și optimizată atât strategic cât și operațional organizația) reprezintă un segment edificator în obținerea unei perspective obiective asupra nevoii de securitate și forma / tipul de abordare de securitate necesar. Înființarea unei structuri de securitate, independentă de celelalte structuri ale organizației reprezintă un pas important spre asigurarea tuturor proceselor organizației. Existența unei astfel de structuri este dovada unei viziuni manageriale, deoarece aceasta nu doar asigură o gestionare bună a problemelor de securitate, dar va avea în permanență ca prim obiectiv protejarea valorilor entității pe care o reprezintă în vederea atingerii scopului organizației, prin protejarea informației în toate formatele sale și asigurarea securității fluxului informațional prin care datele sunt vehiculate.

B. **Cultul muncii** atrage o serie de întrebări fundamentale precum „Care este specificul organizației privind cultul muncii?" sau „Putem vorbi de o cultură de securitate în cadrul organizației?". În baza întrebărilor de acest tip, se pot construi scenarii în ceea ce privește pregătirea personalului în raport cu securitatea informației și securitatea cibernetică.

C. **Conștientizarea și prevenirea** în organizație poate veni sub diverse forme, precum cea a programelor de pregătire, a testelor de securitate, sondajelor sau multe altele. Personalul, datorită progresului tehnologic rapid, poate fi confuz în ceea

persoane şi lucruri gestionate în vederea satisfacerii unei necesități publice de către o colectivitate publică, supuse autorităţii şi controlului acesteia".

1. Prakash Binwal, „Creating a Cybersecurity Governance Framework: The Necessity of Time", iulie 2015, https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/, accesat în data de 22.10.2017.

ce privește *„ce este bine”* și *„ce este rău”* în sectorul securității personale, a securității secretului profesional sau a securității informației manipulate în general. Din păcate, în foarte multe instituții publice și private, deși există un cadru de reglementare a pregătirii continue, forma de pregătire ori este tratată subiectiv și superficial ori nu se face, recurgându-se la o formă de asumare nefondată. În ceea ce privește pregătirea continuă a personalului pe linia securității, lipsa implicării factorului decizional în activitatea de pregătire continuă, formare sau specializare reprezintă unul dintre motivele pentru care în urma unui audit de securitate se reliefează problematica de securitate compusă adesea din lacune în zona de proces a informației, alerte, evenimentele și incidente de securitate cu sau fără intenție, la diferite niveluri de risc și impact asupra organizației. Un astfel de caz este reprezentat în colecția de elemente de acces în clar într-un număr de 1.4 miliarde identificate de către o companie cu profil analitic online, 4IQ (226.631 conturi de administrare de tipul administrator, *„admin”* și *„root”* identificate într-o colecție găsită în *„deep-web”*[1]);

D. **Guvernanța securității cibernetice** joacă un rol extrem de important în realizarea și atingerea obiectivului de securitate a organizației nu numai pentru nevoile actuale, dar, de asemenea, pentru a asigura planuri manageriale de atenuare bine elaborate în vederea rezistenței în fața viitoarelor provocări. Pentru a aborda specific problemele actuale de securitate, cadrul de guvernanță vizează: îmbunătățiri ale politicilor de securitate, aplicarea controalelor tehnice atât metodologic cât și procedural, evaluarea și auditarea sistemelor de securitate /securizare, precum și sensibilizarea oamenilor pentru a-și

1. Julio Casal, „1.4 Billion Clear Text Credentials Discovered in a Single Database”, 9 decembrie 2017, https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14, accesat în data de 03.01.2017.

forma o părere reală și obiectivă și a lua o atitudine adaptată nevoilor identificate și de a dezvolta (chiar instinctiv) o reacție față de comportamentele sigure atât în mediul online, cât și în cel real. Acestea sunt relevante, deoarece ~80% din atacatorii din mediul cibernetic folosesc tehnici de inginerie socială în detrimentul tehnicilor de atac direct asupra echipamentelor electronice și de comunicații[1], exceptând atacurile de tip APT. Pentru provocările ce vor apărea din cauza trendului ascendent al criminologiei cibernetice, cadrul de guvernanță trebuie să se concentreze în permanență asupra factorilor de amenințare emergenți, asupra schimbărilor rapide din peisajul tehnologic, a opiniilor și comportamentului oamenilor raportat la transformările cultului muncii - care suferă o tranziție spre digitalizare - și desigur asupra dezvoltării unei culturi de securitate.

În perioada alocată documentării și cercetării prezentei teme de cercetare, am observat o digitalizare pe un trend ascendent a tuturor domeniilor (*bancar, învățământ și cercetare, fiscal șamd*), fenomen provocat de o nevoie tot mai mare de răspuns la cerere într-un timp cât mai scurt, indiferent de aspecte precum zona geografică sau limbă. Deoarece rezultatele și eficiența sau ineficiența guvernării unui domeniu sunt cuantificate în impact financiar, toate sectoarele guvernate sunt interdependente și sunt sensibile în general la creșterea sau scăderea eficienței - spre exemplu un blocaj al sectorului economic național blochează automat celelalte sectoare, precum educația, transportul, investițiile, militar șamd. Digitalizarea reprezintă un progres extraordinar al societății contemporane, dar exact din acest motiv, anume din lipsa granițelor fixe în mediul virtual, clar delimitate și riguros monitorizate, amenințările cibernetice sunt prezente pretutindeni, atât în sectorul privat (comerț, afaceri, servicii șamd) cât și în sectorul

1. Chris Pogue, „The Black Report", 2016, https://www.nuix.com/sites/default/files/report_the_black_report_web_us.pdf, accesat în data de 03.01.2017.

militar, respectiv în teatrele de operațiuni (*marin, terestru și aerian*) la care în mod natural se adaugă cel informațional și cel cibernetic[1]. Acest lucru nu înseamnă că vulnerabilitățile sunt comune sau că sunt supuse acelorași riscuri. Astfel, doresc să menționez faptul că acest nou areal - spațiul virtual - datorită impactului extraordinar pe care îl are în creșterea capacității militare, a fost recunoscut ca teatru de operațiuni militar de către secretarul general al NATO în iunie 2016 cu referire directă la Articolul 5[2] al NATO. Recunoașterea oficială a spațiului virtual ca „*Noul teatru de operațiuni militar*" nu mai reprezintă un subiect tabu, fiind deja recunoscut în plan internațional atât de organismele politice, militare, publice, cât și de sectorul privat. Impactul pe care îl poate avea utilizarea instrumentelor specifice arealului cibernetic în sectorul militar este dat de capacitățile sporite de acțiune și răspuns care pot fi atinse prin alocarea resurselor minime și posibilitatea de concentrare a forțelor punctual prin atingerea obiectivului militar cu pierderi minime. Cercetarea, inovarea și dezvoltarea în sectorul de apărare a schimbat raportul de investire a resurselor în timp de la planul terestru, la cel maritim, la cel aerian și acum la spațiul virtual, următorul plan de cucerit fiind cel spațial. În contextul global al securității arealului cibernetic, cea mai de dorit resursă este informația, indiferent de forma sa. Trebuie menționat faptul că în mediile virtuale forma vehiculată a informației este electronică - *audio, video, text* - și este transportată prin diverse noduri de comunicații și canale de comunicații precum sunt cablurile submarine - *care aparțin corporațiilor private* - , centre de date, servere – *noduri de comunicații, centre de date, servere de exchange, servere proxy șamd* - , sisteme informatice de comunicații fixe și portabile, echipamente inteligente mobile - *autovehicule, telefoane, tablete, ochelari, ceasuri șamd* - , prognozându-se că în următoarea decadă instrumentul

1. „Cyber defence", 14.12.2017, https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat în data de 03.01.2017.
2. „Collective defence - Article 5", 22.03.2017, https://www.nato.int/cps/en/natohq/topics_110496.htm, accesat în data de 03.01.2017.

dorit și în același timp resursa râvnită de toți va fi reprezentată de sistemele centralizate de IoT dezvoltate pe baza tehnologiei de Inteligență Artificială (AI), puternic propulsată de concepte precum este „*machine learning*" (ML). Inteligența artificială reprezintă o resursă oferită de progresul tehnologiei contemporane cu o capacitate reală de materializare și proiectare a diverselor instrumente utilizate în context defensiv / ofensiv, atât în sectorul militar cât și în sectorul public-privat ori social.

Odată cu recunoașterea spațiului cibernetic ca unul dintre cele cinci arealuri (*terestru, maritim, aerian, spațial și cibernetic*), motivația pretendenților tot mai mare la informație, resurse și tehnologie în continuă evoluție împinge forțe naționale, supranaționale și internaționale să îl îmbrățișeze și să aducă investiții semnificative în cercetare și inovare pentru obținerea unor instrumente utile înțelegerii și guvernării cât mai ecologice și eficiente a spațiului cibernetic. Se poate observa existența unei curse a înarmării cu resurse și instrumente în spațiul cibernetic și chiar o competiție acerbă între state, alți actori non statali și diverse organizații care furnizează soluții de securitate cibernetică. Care sunt aceste forțe și care este rolul acestora în proiecția viitoarelor perspective ale statelor și ale societății în general? Vulnerabilitățile sunt prezente peste tot în organizație, începând cu utilizarea echipamentelor personale ale angajaților în cadrul rețelelor informatice ale organizațiilor și până la utilizarea instrumentelor și aplicațiilor utilizate pentru managementul infrastructurii sau arhitecturii fluxului informațional intern. Desigur, nivelul de risc este rezultat conform implementării strategiei de management a riscului, efectuat cu caracter permanent asupra întregului sistem informatic de comunicații și tehnologie a informației - hardware și software. Rezultatele managementului riscului sunt mult mai evidente în contextul militar ori de afaceri sau pur și simplu în funcționarea infrastructurii de tip IoT în orice mediu. În acest moment este prematur să vorbim despre un sistem/platformă IoT fără cusur, deoarece IoT

reprezintă un risc la adresa utilizatorilor și a organizațiilor prin simpla integrare în acesta a diferitelor componente distribuite în sistemele operaționale sau rețele, prin servicii de tip *Cloud* sau alte tipuri de servici asimilate. În aceeași măsură, o vulnerabilitatea a sistemului informațional este reprezentată de actorul uman care operează sau gestionează oricare dintre serviciile sau activele organizaționale. Drept urmare, este esențial ca fiecare organizație să dețină un cadru bine definit în materie de securitate cibernetică. O dată cu intrarea în vigoare a recomandărilor GDPR[1] în ceea ce privește protecția datelor cu caracter personal, din cauza amenzilor foarte mari, organizațiile au depus un prim efort în acest sens prin reconceptualizarea ecosistemul de securitate IT pentru respectarea obligațiilor evidențiate în legislația internațională și ratificate în cea națională.

La nivelul oricărei organizații, odată cu dobândirea cunoștințelor privind sectoarele de activitate, ale instrumentelor de lucru utilizate de organizație (resurse umane, echipamente, tehnologii șamd.), cunoscând tot ceea ce ține de guvernarea organizației în armonie cu legislația națională și internațională, suntem nevoiți să ne orientăm atenția și spre posibilitatea de extindere a influenței din plan național în cel internațional. Un exemplu extraordinar de parteneriat între sectorul privat și stat în context internațional îl reprezintă promovarea valorilor, produselor și serviciilor organizațiilor prin intermediul resurselor guvernamentale și diplomatice. Un asemenea model este cel japonez, care promovează organizațiile cu capacități de extindere a ariilor de interes prin alocarea de resurse în vederea purtării de discuții bilaterale[2] cu alte state, ceea ce poate facilita parteneriatele operaționale și strategice.

1. GDPR Portal, „Site Overview”, https://www.eugdpr.org/, accesat în data de 03.01.2017.
2. Robert Lupitu, „Klaus Iohannis și Shinzo Abe, anunț de la Tokyo: Parteneriatul Strategic dintre România și Japonia va fi lansat în 2021, la 100 de ani de la stabilirea relațiilor diplomatice”, 21.10.2019, https://www.caleaeuropeana.ro/klaus-iohannis-si-shinzo-abe-anunt-de-la-tokyo-parteneriatul-strategic-dintre-romania-si-japonia-va-fi-lansat-in-2021-la-100-de-ani-de-la-stabilirea-relatiilor-diplomatice/, accesat în data de 07.06.2020.

OBIECTIVE, IPOTEZE ȘI SCOP

Obiectivul general al tezei constă în cercetarea raportului dintre guvernanța securității naționale, reziliența, diplomația, jurisdicția și buna guvernare a spațiului cibernetic de către societatea românească și instituțiile de drept public și privat din România pe o perioadă de cinci ani (2015-2020) în vederea confirmării sau infirmării eficienței și nivelului de securitate ale noilor sisteme informaționale din spațiul virtual.

Din acest obiectiv general face parte și cunoașterea impactului adus de implicarea actorilor non statali și a organismelor de specialitate la nivel național asupra guvernanței spațiului cibernetic în jurisdicția românească, dar și a rezultatelor alinierii conceptelor privind buna guvernare a securității întregului spațiului cibernetic cu setul legislativ și normativ unitar la nivelul Uniunii Europene.

În subsidiar, prin formularea obiectivelor secundare de cercetare, mi-am propus:

Obiectiv Nr. 1. Identificarea implicațiilor aduse de buna guvernanță a securității sectorului cibernetic ca parte integrantă a securității naționale pentru România, în calitate de stat membru al Uniunii Europene.

Obiectiv Nr. 2. Identificarea determinantelor guvernanței securității naționale rezultate în urma adaptării sistemului de management al securității informației în spațiul virtual românesc.

Obiectiv Nr. 3. Studierea paradigmei guvernanței securității informației în spațiul virtual în asentimentul realismului și a supranaționalismului.

În parcursul științific se va încerca demonstrarea validității ipotezei principale de cercetare asupra raportului și impactului relației de interdependență dintre managementul informației și sistemele organizaționale în virtutea securității naționale, iar pe de altă parte de validare a impactului adus de cultura de securitate cibernetică a

cetățenilor din România asupra sistemului de securitate organizațională și securitate națională.

Ipoteza generală de cercetare este dată de existența cuantificabilă a rezultatelor organismelor din România în materie de securitate cibernetică în procesul de validare a bunei guvernanțe în context supranațional. Ipoteza teoretică de cercetare este puternic influențată de nivelul culturii de securitate cibernetică a populației din România. Procesul de cercetare științifică prin culegerea de date în vederea obținerii unei analize cantitative confirmă nivelul de impact adus de nivelul de cultură de securitate cibernetică a populației asupra managementului riscului în organizațiile românești, indiferent de mediul din care acestea fac parte.

Pornind de la ipoteza generală de cercetare, în vederea atingerii obiectivelor propuse, s-a considerat că buna guvernanță în spațiul cibernetic poate să contribuie la soluționarea paradigmei de securitate în acest nou areal, unde organizațiile și statele alocă resurse nesemnificative creșterii securității informației, capacității de răspuns și rezilienței la incidente cibernetice, dar în aceeași măsură pierderile sunt tot mai mari, iar gradul de conștientizare este materializat în majoritatea strategiilor - *strategii de afaceri, Strategia de securitate cibernetică a României, Strategia națională de apărare șamd*.

În aceeași măsură, dilema de securitate cibernetică este dată de alegerea dintre asumarea unui cadru legislativ restrictiv cu impact major asupra liberei circulații a informației sau investirea de resurse în securitatea infrastructurilor care gestionează fluxuri de date și informații a căror valoare cumulată și divulgată neautorizat poate aduce prejudicii organizațiilor publice, private și instituțiilor statului.

Prin metodologia de cercetare științifică abordată voi putea infirma sau confirma existența unei relații de interdependență între practicile de guvernare a sistemelor naționale de securitate a informației și cele supranaționale. Totodată, se va trata și gradul de relaționare dintre sistemele de guvernare a informației în spațiul european.

Ipoteza secundară de cercetare este dată de posibilitatea existenței unei interdependențe între nivelul culturii de securitate a utilizatorilor din România și impactul avut de aceștia asupra dimensiunii securității cibernetice ca subdomeniu al securității naționale.

În cazul de față, adoptând o strategie de cercetare explorativă și orientată spre rezultate concrete, am optat pentru enunțarea distinctă a ipotezelor secundare ale cercetării în cadrul fiecărui capitol în parte.

În vederea obținerii unor rezultate cuantificabile în contextul tratării obiectivelor de cercetare propuse, am considerat potrivit să răspundem următoarelor întrebări de cercetare:

Întrebarea Nr. 1. Care este actualul context de securitate al managementului informației vehiculate în spațiului virtual?

Întrebarea Nr. 2. Care sunt condițiile în care un stat poate să asigure o reziliență cibernetică pentru securitatea națională printr-un management eficient al informației vehiculate în spațiului virtual?

Întrebarea Nr. 3. Care sunt direcțiile de dezvoltare și cercetare a guvernanței securității cibernetice în contextul actualei societăți informaționale din România?

Întrebarea Nr. 4. Care este contextul și nivelul culturii de securitate cibernetică a populației din România?

Ca urmare a recomandărilor obținute la începutul parcursului științific privind alegerea temei, am constatat faptul că interesul comunității științifice față de tema de cercetare propusă și a rezultatelor obținute în urma cercetării acesteia poate fi obținut doar prin identificarea unor noi direcții de cercetare față de literatura de specialitate existentă. Drept urmare, propunerile primite din partea comunității științifice au fost de consolidare a literaturii existente în contrast cu rezultatele unui proces de cercetare bazat pe date concrete și analizate din punct de vedere statistic. Rezultatele obținute în urma acestui parcurs științific se doresc a fi utile în dezvoltarea domeniului de management al securității informației, al guvernanței

securității naționale și actualizarea legislației naționale în raport cu dinamica progresului tehnologic.

Dinamica evenimentelor vehiculate prin intermediul arealului cibernetic, care au avut un impact major asupra statelor, a influențat major[1] comportamentul organismelor internaționale și a guvernelor statelor membre UE cu privire la asumarea responsabilității privind securitate cibernetică în toate sectoarele societății. Acest fapt demonstrează nevoia de percepție și înțelegere a potențialilor factori de risc asupra securității naționale care au loc în mediile spațiului cibernetic.

În ceea ce privește cuvintele cheie[2] identificate și alese, acestea reprezintă elemente definitorii de referință în studiul științelor de securitate și în studiul relațiilor internaționale în societatea contemporană.

Instrumentele de cercetare aplicate în această lucrare sunt necesare pentru a expune și întări într-un mod pragmatic acțiunile desfășurate în mediile virtuale atât ale utilizatorilor, ale managerilor din sectorul privat, cât și ale decidenților din sectorul guvernamental. Pe parcursul perioadei de validare a instrumentelor de cercetare, am identificat din partea corespondenților afiliați sectorului privat din România o lipsă de reacție și interes față de importanța problematicilor de securitate și guvernanță a spațiului cibernetic. Considerăm această teză de doctorat ca fiind rezultatul unui parcurs științific care încearcă să demistifice, printr-o abordare multidisciplinară aflată la intersecția științelor sociale (drept, sociologie, psihologie), științelor exacte (tehnologia informațiilor și a comunicațiilor) și științei securității, un nou subiect integrant al științelor politice și al relațiilor internaționale.

1. Damien McGuinness, „How a cyber attack transformed Estonia", Tallinn, Estonia, 27.04.2017, https://www.bbc.com/news/39655415, accesat în data de 07.06.2020.
2. Cuvinte cheie: *Cultura de Securitate Cibernetică, Realism și Supranaționalism, Guvernanța Securității Cibernetice, Diplomația Spațiului Cibernetic, Reziliența Cibernetică, Buna Guvernanță Cibernetică*

METODOLOGIA ȘI STRATEGIA DE CERCETARE

În selectarea materialelor de cercetare și a resurselor necesare construirii unei strategii de cercetare conforme actualelor standarde academice[1], după realizarea unui instrumentar de evaluare a contextului și nivelului culturii de securitate cibernetică în România, am fost nevoit să mă îndrept preponderent spre literatura de specialitate internațională. Până în prezent majoritatea cercetărilor științifice realizate asupra domeniului cibernetic - mediile digitale și virtuale, fluxurile informaționale, rețelele informatice șamd - au avut ca obiectiv tratarea din perspectiva științelor exacte, pe când din perspectiva relațiilor internaționale, a studiilor de securitate sau diplomatice, cercetarea este dificil de identificat în România. Aceste argumente m-au determinat să mă concentrez asupra literaturii internaționale, unde observăm că metodologiile de cercetare științifică[2] au consacrat diverse tipare, modele de exploatare a cunoașterii științifice. După cum bine se cunoaște, știința ori domeniul de cercetare științifică au avantajul adus de cercetătorii ce o dezvoltă prin politicile de cercetare consacrate ori orientative și standardele infailibile de obținere a rezultatelor. Așadar, concretizarea părții teoretice a tezei va fi validată și prin rezultatele obținute prin aplicarea instrumentelor de cercetare. Aceste instrumente - chestionar, interviu - sunt rezultate în urma consultării opiniilor specialiștilor în sociologie, filosofie și statistică, care și-au adus aportul la alegerea propriilor metode[3] și metodologii[4] de identificare, planificare spre colectare, inventariere, analiză și sinteză a datelor.

1. Norman Blaikie, *Modele ale cercetării sociale: Producerea cunoașterii*, Ediția a II-a, (trad. Coca Vieru, Ana Gruia), Ed. CA Publishing, Cluj-Napoca, 2010, p.10.
2. *Ibidem*, pp.11, 75.
3. *Metode complexe care utilizează instrumente specifice procesului de precofigurație a unor posibile soluții și testarea acestora în contextul tehnicilor și procedurilor de analiză și sinteză a datelor din teren privind dilema de securitate cibernetică.*
4. *Metodologii proprii de cercetare la care s-au alăturat cutuma, recomandarea, directiva ori regulamentul generat și validat în parcursul epistemologic al ante-cercetătorilor noștri.*

Pentru a demistifica intenția autorului, în acest caz se consideră potrivită și necesară interpretarea rezultatelor obținute prin metodele de cercetare alese, pentru a obține cea mai bună soluție și o perspectivă de dezvoltare a rezultatului obținut în urma cercetării științifice prin tema abordată într-un demers de talia unei teze de doctorat în arealul cunoașterii științifice fundamentale în domeniul relațiilor internaționale.

Față de cele mai sus menționate, optăm pentru alegerea unor soluții metodologice specifice interdisciplinare din domeniul relațiilor internaționale și științelor europene, cu preponderență în arealul relațiilor internaționale și studiilor de securitate. Metodologia de cercetare este construită pe marginea studierii practicilor unei bunei guvernanțe în spațiul cibernetic. Totodată, putem observa că determinantele rezilienței cibernetice - pilon important al guvernării spațiului cibernetic - sunt puternic influențate de dezvoltarea unei noi forme a diplomației, cunoscută deja ca diplomație cibernetică. În acest context general, statele, prin acțiunile de întărire a relațiilor internaționale, depun eforturi considerabile în vederea respectării limitelor jurisdicționale (*naționale și internaționale*).

Pe parcursul cercetării au fost utilizate două metode de cercetare.

Metoda de cercetare aleasă în cazul studiului de caz este bazată pe aplicarea principiilor modelului corelațional explicativ, unde presupunem că cercetarea are obiectivul de a descoperi în ce măsură variabilele prezintă o variație reciprocă. Datele sunt evaluate transversal de îndată ce acestea au fost centralizate și validate. Detalierea metodologiei de lucru și procesul de analiză statistică cantitativă sunt evidențiate în capitolul dedicat studiului de caz. În această ordine de idei, pentru a preveni și înlătura erorile de analiză cantitativă și pentru a emite o formulare fidelă realității, putem afirma că analiza calitativă va fi concentrată în concluziile autorul din finalul tezei.

În vederea obținerii unor rezultate de necontestat și validate de o autoritate recunoscută în domeniul analizei statistice, am solicitat

susținerea Universității din Gröningen[1]. Am apelat la această opțiune din motive obiective, precum: limitările de ordin financiar, neidentificarea unor specialiști disponibili și autorizați în analiza statistică, lipsa echipamentelor și aplicațiilor specifice și necesare obținerii unor rezultate relevante. Sentimentul de încredere din partea conducerii institutului s-a materializat prin încheierea unui parteneriat, în urma căruia mi-au pus la dispoziție expertiza propriilor specialiști[2],[3] în analiză statistică și psihometrie pentru a mă îndruma în procesul de analiză statistică cantitativă a datelor culese cu ajutorul echipamentelor și programelor pentru analiză statistică, cum sunt **R** (*R programming language for statistical computing;* ***R***[4] ***Core Team 2019*** *și* ***SPSS***[5] ***v.25***.

Întregul proces de cercetare este un efort susținut al autorului, care își asumă utilizarea instrumentarului de analiză a datelor culese prin aplicarea chestionarelor și utilizarea altor resurse necesare obținerii de rezultate concludente în procesul de analiză cantitativă a datelor[6] și desigur a emiterii de concluzii bazate pe analiza calitativă a acestora.

Metoda studiului de caz în prezenta lucrare este în mod special realizată prin aplicarea principiilor modelului corelațional explicativ, cu mențiunea că, pentru a crea o plasă de siguranță în ceea ce privește

1. Universitatea din Gröningen – Institutul de Psihologie Heymans – Departamentul de Psihometrie și Statistică, Gröningen, Olanda.
2. Prof. univ. dr. R.R. (Rob) Meijer, Directorul Departamentului de Psihometrie și Statistică, – Institutul de Psihologie Heymans – Universitatea din Gröningen.
3. Asist. univ. drd. Daniela Crișan, Departamentul de Psihometrie și Statistică, – Institutul de Psihologie Heymans – Universitatea din Gröningen.
4. R Core Team, „R: A language and environment for statistical computing", R Foundation for Statistical Computing, Vienna, Austria, https://www.R-project.org/, accesat în data de 19.03.2019.
5. IBM Corp. (2017), „IBM SPSS Statistics for Windows - Statistical Package for Social Sciences", Version 25.0, Armonk, NY: IBM Corp, https://www-01.ibm.com/support/docview.wss?uid=swg24043678, accesat în data de 19.03.2019.
6. Jonathan Grix, *Demistificarea cercetării postuniversitare: De la masterat la doctorat*, (trad. Nicolae Melinescu), Ed. CA Publishing, Cluj-Napoca, 2014, pp.26-27.

validarea rezultatelor, s-a utilizat și metoda de verificare încrucișată, unde s-a testat și verificat experimental valoarea teoretic-aplicativă a rezultatelor de cercetare obținute de pe urma cercetării temei propuse.

Înaintea aplicării chestionarelor s-a parcurs un proces de verificare și validare a principalului instrument de culegere a datelor din teren, chestionarului. Pentru întocmirea formei chestionarului și pentru crearea setului de întrebări cu diverse forme de răspuns, autorul a făcut apel la practicienii din arii de expertiză diferite - psihologie, psihometrie, sociologie, management și IT&C.

Din rațiuni de echidistanță academică și echilibru, am avut în vedere respectarea următoarelor principii fundamentale de cercetare:

- √ **principiul explorării și al descrierii fenomenelor** - lucrarea s-a axat pe un studiu explorativ, anume pe descrierea și explorarea relațiilor dintre fenomene;
- √ **principiul corespondenței** - rezultatele au fost bazate pe o permanentă racordare la cunoașterea academică și științifică contemporană;
- √ **principiul observabilității** - pe parcursul lucrării s-au expus rațional argumente ce pot fi verificabile cel puțin la nivel cognitiv.

Nu în ultimul rând, activitățile de observare, cercetare și analiză s-au axat în principal pe:

a. **aplicarea de interviuri** bazate pe rezultatele chestionarelor obținute în cursul cercetării;

b. **consultarea unor practicieni din domeniu sau din domenii conexe** - atât în cadru formal (*conferințe tematice, manifestări științifice*), cât și informal (e-*mail, videoconferințe, telefonic sau în cadrul forumurilor specializate disponibile online*);

c. **studierea documentelor primare** - obiectivul general de cercetare a fost conturat în baza analizării surselor bibliografice. Dintre acestea amintesc: rapoarte ale organizațiilor guvernamentale/nonguvernamentale, rapoarte ale centrelor de

analiză și statistică, analize și rapoarte de cercetare, teze de disertație și doctorat (*din țară și din străinătate*), lucrări științifice[1] prezentate în cadrul manifestărilor științifice, reviste și articole tematice indexate BDI, publicații online, manuale, standarde, ghiduri și proceduri șamd.;

d. **studierea documentelor secundare** - a presupus culegerea de titluri și nume de autori de lucrări relevante din cadrul bibliografiilor și indexurilor digitale disponibile în format IEEEXplore Digital Library[2], Zotero Library[3] șamd;

e. **studierea documentelor terțiare** - a presupus culegerea și analizarea de surse bibliografice cu grad ridicat de veridicitate, abstractizare și potențial de valorificare, precum: rapoarte, sinteze și documente guvernamentale declasificate ca urmare a unor scurgeri de informații, alte documentele declasificate sau literatură[4] „gri"[5];

În procesul de generare de materiale vizuale au fost folosite și aplicații informatice secundare, ca spre exemplu generatoarele de hărți relaționale, precum cel utilizat în conceptualizarea relațiilor între ariile de cercetare atinse, „*The Brain*" și cel utilizat în crearea de hărți relaționare complexe, „*IBM i2 Analyst's Notebook*". Pentru interpretarea statistică cantitativă, s-au utilizat aplicațiile de interpretare a datelor statistice și de generare a rapoartelor statistice „*R*" și „*IBM SPSS Statistics for Windows*".

La finalul completării chestionarelor s-au adresat întrebări de lămurire pentru verificarea încrucișată a răspunsurilor deja furnizate în formular. Datorită necesității de a cuantifica eficient rezultatele obținute în urma cercetării cantitative și calitative, s-a considerat propice utilizarea metodei observației ca modalitate de studiu a cazuisticii pe

1. Richards J. Heuer Jr., *Psychology of Intelligence Analysis*, Ed. CIA Center for the Study of Intelligence, 1999.
2. IEEE Xplore Digital Library, https://ieeexplore.ieee.org, accesat în data de 21.11.2016.
3. Zotero, https://www.zotero.org/, accesat în data de 21.11.2016.
4. Literatura „gri", http://www.greylit.org/about, accesat în data de 29.05.2018.
5. Literatura „gri", http://www.opengrey.eu/about/greyliterature, accesat în data de 29.05.2018.

întreg parcursul științific. În acest context, scheme logice generate, notițele scrise și graficele, precum și studiul bibliografiei au fost gestionate în sisteme de tip „*cloud*”[1], prelevate și din sisteme de culegere de informații din surse deschise precum este Klarmedia[2] și Statista[3] sau baze de date internaționale electronice „*Mendeley*”, „*O'Reilly*”, „*Safari*”, „Archive.org”, respectiv „*IEEE Xplore Digital Library*”.

METODE ȘI TEHNICI	PROCEDEE	INSTRUMENTE
Metoda aplicării principiilor modelului corelațional explicativ	centralizarea datelor; calculul și analiza datelor; rapoarte de analiză cantitativă; grafice.	The Brain, R (*R programming language for statistical computing*); R Core Team 2019, SPSS v.25, OneDrive
Metoda observațiilor	scheme logice; notițe scrise și grafice; studiul bibliografiei.	MsOffice, OneDrive, TheBrain, Mendeley, O'Reilly, Safari, Archive.org, Statista, Klarmedia, IEEE Xplore Digital Library
Metoda studiului de caz	notițe scrise; studiul bibliografiei.	MsOffice, OneDrive, Mendeley, O'Reilly Safari, Archive.org, Statista, Klarmedia, IEEE Xplore Digital Library

Tabelul nr.1 - *Metode, tehnici, procedee și instrumente de cercetare utilizate*

1. OneDrive, https://login.microsoftonline.com/, accesat în data de 25.05.2018.
2. Klarmedia, https://www.klarmedia.ro/#media-monitoring, accesat în data de 25.05.2018.
3. Statista, https://www.statista.com/markets/, accesat în data de 25.05.2018.

Motivația alegerii temeii de cercetare

Alegerea unei teme de cercetare concludente pentru actualul context de securitate internațional, european și românesc a fost motivată în primul rând de dorința autorului de a valorifica în plan științific experiența profesională acumulată pe parcursul a peste paisprezece ani de activitate în domeniul TIC și a securității cibernetice. Motivația principală mai sus menționată a fost susținută și de identificarea unei posibilități de a materializa experiența profesională aliniată cunoștințelor teoretice din domeniul managementului informației, guvernanței și diplomației spațiului virtual, relațiilor internaționale și a studiilor europene. O importanță deosebită în alegerea temei au avut limitările de ordin tehnic apărute în urma studierii managementului securității informației, cu precădere în urma analizei ciclului de viață a informației, de la strângerea datelor în format fizic sau digital la emiterea informației, gestionarea și vehicularea acesteia în mediile virtuale și până la arhivarea sau distrugerea acesteia.

Într-un mod absolut natural, în urma experienței profesionale consolidată de studiile de securitate, am identificat necesitatea de a cerceta sectorul securității și guvernanței spațiului cibernetic, deoarece aceste domenii reprezintă o arie prioritară de cercetare și inovare, cel puțin din perspectiva dezvoltării durabile a spațiului cibernetic.

Această nevoie am identificat-o ca fiind evidențiată în România de existența lacunară a cercetărilor științifice orientate pe securitate cibernetică din prisma relațiilor internaționale. Necesitatea anterior menționată există și datorată numărului foarte scăzut de cercetătorilor români orientați spre identificarea și tratarea ori soluționarea situațiilor specifice relațiilor internaționale și studiilor de securitate în general ori de nișă în arealul spațiului cibernetic. Acest lucru duce la o limitare a capacității de reziliență și răspuns pentru sistemului de apărare și securitate românesc contemporan în fața potențialelor amenințări. În fapt, această nevoie evidențiază privarea sistemului de securitate națională de resursele de securitate strategice, atât de necesare azi unui stat cu ambiții euroatlantice considerabile cel puțin în domeniul securității cibernetice. Pe considerentul că cercetările științifice orientate înspre managementul securității cibernetice reprezintă o etapă determinantă în managementul spațiului cibernetic ca și a capacității de răspuns în fața potențialului factor de risc apărut sau generat în arealul cibernetic global, din perspectiva relațiilor internaționale, acest domeniu de cercetare reprezintă unul dintre pilonii principali ai dezvoltări sistemului de securitate națională.

Alegerea temei de cercetare a fost motivată într-o mare măsură de tendința UE de dezvoltare a mecanismelor de securitate și guvernanță a spațiului cibernetic, fiind de asemenea evidențiată ca subiect prioritar pe agenda comunității europene. În procesul de documentare, autorii români nu s-au remarcat prin realizări științifice marcante, motiv pentru care am fost nevoit să citez și să analizez autori consacrați în acest domeniu din mediul internațional. În etapa de structurare pe capitole și subcapitole a tezei, pentru a se putea realiza un studiu specific și individual pentru fiecare subiect, am ales principiul separării capitolelor pe tematici distincte. În acest context, concluziile preliminare ale capitolelor scot în evidență rezultatele obținute pentru a răspunde la întrebările de cercetare emise și pentru a înțelege interdependența, cel puțin la nivel teoretic, dintre științele

relațiilor internaționale și studiilor de securitate, științele juridice de drept național și internațional, managementul securității informației în spațiul cibernetic și a importanței culturii de securitate cibernetică a persoanelor active în mediul virtualizat online sau offline. Motivația acestei construcții a fost dată de necesitatea de raportare și concentrare a procesului de cercetare pe domeniul de studiu al autorului, anume cel al relațiilor internaționale și studiilor europene.

În măsura în care interesul privind guvernanța spațiului cibernetic crește pentru toți actorii din spațiul internațional, guvernanța acestui sector devine un element de o deosebită importanță în ceea ce privește securitatea națională. Leitmotivul acestei teze este dat de înțelegerea nevoii de guvernanță și management elitist al securității spațiului virtual în relație cu principiile realismului comparat cu tendințele supranaționaliste resimțite la nivel global, de la simpla utilizare a unui terminal informatic până la a aborda strategii diplomatice cu impact mondial.

Cuvinte cheie

TERMEN	**EXPLICAȚII**
Cultura de Securitate Cibernetică	Definim cultura de securitate ca un efort colectiv, coordonat sau identificat la toate nivelele sociale, apărut în contextul digitalizării mediilor societății contemporane și motivat de nevoia de reziliență cibernetică și/sau mitigare a pericolelor (riscuri, vulnerabilități șamd.) provenite din și în arealul cibernetic.
Realism și Supranaționalism	În actualul context de securitate, managementul informației digitale sau digitalizate, vehiculat în mediile virtuale, primește valori diferite cu un puternic impact decizional. Analizarea capacității de gestionare a acestor resurse în sistemele informaționale naționale, din perspectiva aplicată a ideologiilor realismului față de simularea acelorași capacități și resurse în context supranaționalist, este cu adevărat vitală pentru asigurarea securității naționale la un nivel ridicat.

Pe parcursul întregii teze, se poate observa o perspectivă obiectivă și un studiu comparativ raportat la cele două ideologii aplicate și/sau aplicabile în contextul internațional din care România face parte.

Guvernanța Securității Cibernetice

În sensul lucrării de față, guvernanța securității cibernetice presupune *starea de funcționare optimă ca urmare a aplicării unei guvernări coerente în sectorul tehnologiei informației și a comunicațiilor precum și a managementului eficient prin politizarea teoriilor contemporane de management în politici de securitate funcționale, măsuri pro active și reactive* asupra întregului ciclu de viață a informației în spațiul cibernetic, cu obiectiv principal de protejare a triadei *confidențialitate - integritate - disponibilitate și autenticitate a informațiilor*[1] sintactice și semantice stocate, manipulate în mediul virtual; rezultatele sunt necesar a fi activate în mobilizarea sistemelor de conștientizare, prevenție, diagnoză, reacție, recuperare și continuitate, acestea reprezentând valorile fundamentale ale celui mai valoros bun al organizației, omul.

Diplomația Spațiului Cibernetic

a. strategie de abordare a contextelor diplomatice în plan internațional, care promovează o infrastructură informațională și de comunicație deschisă, interoperabilă, sigură și fiabilă, *„care să sprijine comerțul internațional, să consolideze securitatea națională/internațională și să promove-*

1. U.S. National Security Presidential Directive / NSPD-54, p.3, https://fas.org/irp/offdocs/nspd/nspd-54.pdf, accesat în data de 10.11.2017.

ze libertatea de expresie și inovație, susținând în același timp parteneriatele sustenabile și aplicarea legii în spațiul cibernetic"[1],

b. mecanism național sau internațional cu rol de protejare a suveranității, normelor internaționale și principiilor statului de drept, dar și arbitru în procesul de asigurare a echilibrului între jurisprudența și aplicabilitatea dreptului internațional în raport cu dreptul național, cu aplicabilitate în sectorul infrastructurii tehnologiei informației și a comunicațiilor pe teritoriul național și internațional.

Reziliența Cibernetică

Reziliența în sectorul cibernetic este *de facto*, abilitatea, respectiv *capacitatea de furnizare a* continuității *(proceselor) în obținerea* rezultatului dorit*, în ciuda* evenimentelor cibernetice adverse *(incidentelor cibernetice)*, această definiție este descrisă și justificată în mod sistematic; aici abilitatea este gradată pe șase nivele și este dată de coeficienții de raportare, precum cei naționali, organizaționali sau specifici, în sectorul tehnologiei informației.

Continuitatea face referire la capacitatea de furnizare a rezultatul dorit și atunci când mecanismele uzuale eșuează din motive precum crizele de funcționalitate sau breșele de securitate; acest termen face referire și la recuperarea unui sistem după un eveniment nedorit, dar și la posibilitatea dată de dinamismul sistemului pentru a schimba

1. Cyber Diplomacy Act of 2017, 115th CONGRESS 2d Session https://www.congress.gov/bill/115th-congress/house-bill/3776/text, accesat în data de 04.01.2018.

și modifica sau actualiza - completa - aceste mecanisme în vederea confruntării viitoarelor riscuri.

Rezultatul dorit poate fi definit ca fiind rezultatul pe care vor să îl atingă țările, organizațiile sau sistemele tehnologiei informației (obiective fundamentale ale organizațiilor sau a proceselor instituționale, respectiv forma finală a serviciilor oferite de sistemele de servicii online).

Incidentele cibernetice adverse sunt cauzate de diverși factori interni sau externi din diverse medii, dar care au un impact negativ asupra disponibilității, integrității sau confidențialității sistemelor informatice, informației sau serviciilor din mediile virtuale[1].

Buna Guvernanță Cibernetică

În lucrarea de față, prin bună guvernanță în spațiul cibernetic se înțelege totalitatea politicilor, strategiilor și mijloacelor implementate în mod echilibrat în sprijinul securității, democratizării, prosperității și dezvoltării durabile a spațiului cibernetic.

CUVINTE CHEIE: *Cultura de Securitate Cibernetică, Realism și Supranaționalism, Guvernanța Securității Cibernetice, Diplomația Spațiului Cibernetic, Reziliența Cibernetică, Buna Guvernanță Cibernetică.*

1. Björck F., Henkel M., Stirna J., Zdravkovic J., „Cyber Resilience – Fundamentals for a Definition", în *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, Rocha A., Correia A., Costanzo S., Reis L. (eds), vol. nr. 353, Ed. Springer, Cham, 2015, pp.311-312.

Glosar de abrevieri și acronime

A

APT - Advanced Persistent Threat (trad. *Amenințare Persistentă Avansată*)

AI4EU – Artificial Intelligence for Europe Union (trad. *Inteligență Artificială pentru Uniunea Europeană*)

ANSSI – Asociația Națională pentru Securitatea Sistemelor Informatice

B

BI – Business Intelligence

C

CECO – Comunitatea Europeană a Cărbunelui și Oțelului

CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence (trad. *Centrul de Excelență al Centrului de Cooperare Internațională de Apărare al NATO*)

CCDP – Civilian Capability Development Plan (trad. *Planul de dezvoltare a capacităților civile*)

CCTA – Central Communication and Telecommunication Agency (trad. *Agenția <<britanică>> Centrală de Comunicații și Telecomunicații*)

CAE – Consiliul Afacerilor Externe

CARD – Coordinated Annual Review on Defence (trad. *Coordonat de revizuire privind apărarea*)

CDMB – NATO Cyber Defence Management Board (trad. *Comitetul NATO de Management al Apărării Cibernetice*)

CDP – Capability Development Plan (trad. *Planul de dezvoltare a capacităților*)

CERT – Computer Emergency Response Team (trad. *Echipa de Răspuns la Urgențe de Securitate Cibernetică*)

CEDO – Curtea Europeană a Drepturilor Omului

CI – Competitive Intelligence

CIA – Central Intelligence Agency (trad. *Agenția Centrală de Informații a Statelor Unite ale Americii*)

CIJ – Curtea Internațională de Justiție

CNI – Comunitatea Națională de Informații

CNSC – Centrul Național de Securitate Cibernetică

CoE – Council of Europe (trad. *Consiliul Europei*)

COSC – Consiliul Operativ de Securitate Cibernetică

COMPUSEC – Computer Security (trad. *Securitatea Calculatoarelor*)

C–PROC – Cybercrime Programme Office (trad. *Oficiul Regional pentru Combaterea Criminalității Informatice*)

CRAMM – CCTA Risk Analysis and Management Methodology (trad. *Analiza de Risc și Metodologia Managementului CCTA*)

CSAT – Consiliul Suprem de Apărare a Ţării

CSIRT – Computer Security Incident Response Team (trad. *Echipa de Răspuns la Incidente de Securitate Cibernetică*)

CYBERINT – Cyberintelligence (trad. aprox. *colectare de date și informații din surse cibernetice*)

CYBERSEC – Cybersecurity (trad. *securitate cibernetică*)

D

DEEP–WEB – Parte componentă (96%) a internetului (World Wide Web) care nu poate fi indexată cu ajutorul motoarelor de căutare uzuale și care poate fi accesată prin canale securizate de comunicații, prin intermediul paginilor / portalurilor de acces dinamice și criptate.

DDoS – Distributed Denial–of–Service Attack (trad. *atacuri distribuite de negare a serviciilor*)

E

EDA – European Defence Agency (trad. *Agenția Europeană de Apărare* / AEA)

EDF – European Defence Fund (trad. *Fondul european de apărare*)

ENISA – European Network and Information Security Agency (trad. *Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor*)

EFMS – European Forum for Member States (trad. *Forumul European pentru Statele Membre*).

EFTA – European Free Trade Association (trad. *Asociația Europeană a Liberului Schimb* / AELS).

EC3 – European Cybercrime Centre (trad. *Centrul pentru Combaterea Criminalității Informatice*).

EUROJUST – *„Eurojust supports judicial coordination and cooperation between national authorities to combat terrorism and serious organised crime affecting more than one EU country"*[1] (trad. *„Eurojust sprijină coordonarea și cooperarea între autoritățile naționale, pentru a le ajuta să combată terorismul și formele grave de criminalitate organizată care afectează cel puțin două țări din UE."* [2])

1. EUROPA.EU, About EU, Eurojust, https://europa.eu/european-union/about-eu/agencies/eurojust_en, accesat în data de 27.04.2019.
2. *Ibidem*.

G

GEOINT – Geospatial Intelligence (trad. *Intelligence geo–spațial*)

GCHQ– British Government Communications Headquarters (*trad. Centrul de Comunicații și Internet al Serviciilor de Informații din Marea Britanie*)

H

HNS – Sistemului Național britanic de Sănătate

HRVP – High Representative of the Union for Foreign Affairs and Security Policy / Vice–President of the European Commission *(trad. Înaltul Reprezentant al Uniunii Europene pentru afaceri externe și politica de securitate / vicepreședinte al Comisiei Europene)*

HUMINT – Human Intelligence (trad. aprox. *colectare de date și informații prin surse umane*)

I

ICIN – Infrastructură Cibernetică de Interes Național.

INFOSEC – Information Security (trad. *securitatea informațiilor*)

INT – intelligence (trad. aprox. *informații*)

IoT – Internet of Things (trad. *„Internetul Lucrurilor"*)

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission (trad. *Organizația Internațională pentru Standardizare/Comisia Internațională pentru Electrotehnică*)

ITU – International Telecommunication Union (trad. *Uniunea Internațională a Telecomunicațiilor*)

J

JISR – Joint Intelligence, Surveillance and Reconnaissance in NATO (trad. *Sistemul Întrunit de Intelligence, Supraveghere și Recunoaștere*)

M

ML – Machine Learning (trad. *sistem informatic de inteligență artificială pentru învățare automată*)

MNCD – Multinational Cyber Defence (trad. *Apărare Cibernetică Multinațională*)

MNCD2 – Multinational Cyber Defence Capability Development *(trad. Proiectul Multinațional de Dezvoltare a unor Capabilități)*

N

NATO – North Atlantic Treaty Organization (trad. *Organizația Tratatului Atlanticului de Nord*)

NCI – NATO Communication and Information Agency (trad. *Agenția NATO de Comunicații şi Informații*)

NCIRC – NATO Computer Incident Response Capability (trad. *Capacitatea de Răspuns la Incidente Informatice din cadrul NATO*)

NCCIP – National Cybersecurity and Critical Infrastructure Protection Act (trad. *Actul privind securitatea națională în spațiul cibernetic și protecția infrastructurilor critice*)

NIS – Network and Information Security (trad. *Securitatea Rețelelor și Informației*)

NSA – National Security Agency (trad. *Agenția Națională de Securitate a Statelor Unite ale Americii*)

O

ONU – Organizația Națiunilor Unite

OPSEC – Operations security (trad. *securitatea operațiilor)*

OSCE – Organizația pentru Securitate și Cooperare în Europa.

OSINT – Open–Souce Intelligence (trad. *Intelligence din surse deschise de informații*)

P

PESCO – Permanent Structured Cooperation (trad. *cooperarea structurată permanentă*)

PIB – Produs Intern Brut
PSAC – Politica de Securitate și Apărare Comună

R

RANSOMWARE – Cod/Script/Aplicație malițioasă care se manifestă prin blocarea sistemelor de operare utilizate de victime sau criptarea datelor acestora. Motivul lansării unei astfel de aplicații este unul de șantajare a victimei, de solicitare nelegitimă a unei răscumpărări pentru ca deținătorul datelor sau a sistemului să poată intra din nou în posesia datelor criptate.
RPC – Republica Populară Chineză

S

SCADA – Supervisory Control and Data Aquisition (trad. *Sistem de Monitorizare, Control și Achiziție a datelor*)
SIGINT – Signals Intelligence (trad. *Intelligence din interceptarea semnalelor digitale*)
SNAC – Sistemul Naţional de Alertă Cibernetică
SNAP – Strategia Națională de Apărare
SNSC – Sistemul Naţional de Securitate Cibernetică
SRA – Structured Risk Analysis (trad. *Analiza de Risc Structurată*)
SRI – Serviciul Român de Informații
SSCR – Strategia de Securitate Cibernetică a României
SUA – Statele Unite ale Americii

T

TIC – Tehnologia Informației și Comunicațiilor

U

UE – Uniunea Europeană
US–CERT – United States Computer Emergency Readiness Team (trad. *Centrul de Răspuns la Incidente de Securitate Cibernetică al Statelor Unite ale Americii*)

Capitolul I.
Introducere

Subiectul prezentei teze reprezintă o continuare firească a cercetărilor introductive și aparent eclectice pe care autorul le-a întreprins pe durata studiilor de masterat, urmate în domeniul studiilor de drept și în domeniul studiilor de management al securității în societatea contemporană. Încă de la început, autorul urmărește să-și consolideze poziția științifică și volumul de cunoștințe necesare construirii unei teze de doctorat în managementul informațiilor vehiculate în mediul electronic și a bunei guvernanțe a arealului cibernetic.

Argumentul și expunerea de motive stau la baza acțiunii autorului de a demistifica raportul dintre securitatea cibernetică în calitate de parte componentă a securității naționale cu practica managementului informațiilor vehiculate în arealul cibernetic românesc și european. Pe parcursul tezei, se va observa faptul că această acțiune devine un real proces de validare sau invalidare a întrebărilor de cercetare. Autorul va încerca pe parcursul tezei să identifice dependența sau interdependența dintre securitatea națională și buna guvernanță a spațiului cibernetic, aplicabilitatea conceptelor realismului și supranaționalismului în ceea ce privește trasarea limitelor acțiunilor

actorilor statali și non statali, diplomația cibernetică și diplomația digitală. Un aspect aparte îl reprezintă tratarea dependenței securității cibernetice ca subdomeniul al securității naționale cu cultura de securitate a populației.

Viziunea autorului stă în asumarea procesului de cercetare prin identificarea obiectivului general al tezei, care constă în cercetarea raportului dintre elemente precum guvernanța securității naționale, reziliența, diplomația, jurisdicția și buna guvernare a spațiului cibernetic, în vederea confirmării sau infirmării tipologiilor și noilor sisteme informaționale din spațiul virtual precum și al aportului adus de acestea în balanța guvernanței spațiului virtual între realism și supranaționalism.

Ipotezele sunt emise în urma unui îndelung proces de documentare și în baza interesului specific din partea comunității științifice față de tema de cercetare propusă, orientat pe înțelegerea nevoii de cercetare și inovare în domeniul managementului securității informației, guvernanței securității naționale și actualizării legislației naționale în raport cu dinamica progresului tehnologic. Pe de altă parte, în subsidiar, ipotezele de lucru sunt emise și în urma studierii dinamicii evenimentelor vehiculate în arealul cibernetic care influențează major evenimentele sociale și politice care au loc în circumscripția UE. Astfel, ipotezele sunt specific restrânse la întrebările de cercetare primare și secundare mai sus enunțate.

Pentru a îndeplini condițiile de formă și conținut ale unui studiu științific obiectiv și cerințele academice de concepere a unei lucrări de cercetare valoroase, autorul a considerat necesară conceperea unei strategii de realizare a cercetării, ceea ce a necesitat, pe parcursul anilor, investigații empirice ale fenomenelor particulare, în contextul de securitate contemporan real şi utilizarea multiplelor surse de informații (*documente, interviuri și chestionare*)[1]. Reiterăm faptul că autorul

1. Robert K. Yin, *Case Study Research: Design and Method*, Ediția a-V-a, Ed. SAGE Publications, California, Thousand Oaks, 2014, pp. 196-200.

se concentrează și asupra identificării unei relații de dependență sau interdependență între nivelul culturii de securitate cibernetică a populației rezidente în România și securitatea cibernetică ca parte componentă a securității naționale. De la această necunoscută, se dezvoltă un mecanism de evaluare a populației, a cărui eșantion, metodologii de lucru și desfășurări sunt exhaustiv explicate în capitolul alocat studiului de caz asupra culturii de securitate cibernetică în România. De menționat este faptul că, în perioada 2016-2018, a aplicat un număr de aproximativ 7.600 chestionare, care reprezentau la momentul centralizării datelor ~0.03% din totalul de 19.644.350 persoane aflate în evidențele Institutului Național de Statistică, conform Breviarului Statistic al INS din 2018. Datorită caracterului sensibil al subiectului de cercetare, autorul a decis ca persoanele care activează în instituțiile de apărare, ordine publică și securitate națională din România să nu fie chestionate. Totodată, autorul a consultat/intervievat specialiști și experți în domeniile de interes ale prezentei teze, atât din sectorul administrației publice și guvernamentale, cât și din mediul privat.

Această strategie de cercetare s-a validat în urma aplicării chestionarelor și interviurilor, respectiv a consultării literaturii de specialitate și interpretării datelor culese. Strategia de cercetare nu s-a concentrat pe analiza de detaliu și construcția instituțiilor naționale din România reprezentative în tratarea subiectului securității naționale și a managementului informației digitale vehiculate în cadrul acestora. Deși există posibilitatea de a apărea confuzia că această cercetare este una mai mult eclectică, orientată spre general, autorul consideră necesară abordarea tuturor particularităților contextuale ale cercetării, unde studiul de caz și analiza statistică reprezintă două dintre instrumente esențiale utilizate în procesul de obținere a unor rezultate corecte și inteligibile[1] în domeniul de studiu al relațiilor internaționale și al studiilor de securitate.

1. Colin Robson, *Real World Research: A resource for Social Scientists and Practitioner-Researchers*, Ediția a-II-a, Ed. Blackwell Publisher, Oxford, 2002, pp. 177-186.

Aceste particularități contextuale ale cercetării sunt reprezentate în primul rând de aplicabilitatea și limitările sistemelor de management al informațiilor vehiculate în mediile virtuale, a guvernanței spațiului cibernetic, a influențelor conceptelor realismului și supranaționalismului asupra sistemului de securitate națională, a formelor diplomației aplicate în arealul cibernetic european sau global și înțelegerea influențelor unei politici unitare europene privind securitatea informației electronice în actuala stare geopolitică globală. În al doilea rând, cunoscând și acceptând că *„în politica de securitate națională trebuie să gestionezi acele evoluții, acele probleme care pot genera rapid crize de securitate națională, care în decurs de zile sau chiar ore, îți pun în pericol integritatea teritorială, suveranitatea, siguranța unui mare număr de oameni"*[1], trebuie acceptate și dovezile care expun vulnerabilitățile[2] sectorului securității naționale în fața atacatorului, datorate lipsei de cultură de securitate a populației[3].

În viziunea autorului, rezultatele acestei cercetări a particularităților contextuale enumerate se verifică într-o nouă lumină prin studiul de caz orientat către o evaluare a ponderii dintre securitatea națională și cultura de securitate cibernetică a populației din România pentru asigurarea unui climat de securitate general.

Studiul de caz, fiind unul complex, a fost realizat prin adoptarea unui set de metode complementare de culegere a datelor, analiză a acestora, prelucrare şi gestionare a informațiilor prelevate, cât și de stocare a informațiilor relevante obiectivelor cercetării. Pentru a obține un set de date cât mai fidel realității, autorul a solicitat sprijinul *„Departamentului Psihometrie și Statistică"* din cadrul *„Facultății de*

1. Iulian Fota, https://www.facebook.com/iulian.fo.1/posts/727760317720639, accesat în data de 27.08.2020.
2. Rain Ottis, „Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accesat în data de 27.08.2020.
3. NATO STRATCOM COE, Cyber Operations, „2007 cyber attacks on Estonia", pp.52-69, https://www.stratcomcoe.org/download/file/fid/80772, accesat în data de 27.08.2020.

Științe Comportamentale și Sociale" a Universității din Groningen, care i-a acordat avizul de încredere, urmat de încheierea unui parteneriat prin care autorul a avut acces la resursele institutului și la expertiza specialiștilor în analiză statistică și psihometrie, care l-au îndrumat în procesul de analiză statistică cantitativă a datelor culese cu ajutorul echipamentelor și programelor pentru analiză statistică, cum sunt ***R**, **R Core Team 2019** și **SPSS v.25***. În acest context, este important de menționat faptul că rezultatele cercetării sunt în totalitate obținute din activitatea științifică a autorului.

În procesul documentării și identificării câmpului empiric de cercetare, autorul a recurs la aprofundarea și studierea diferențelor dintre metodele de guvernare ale arealului cibernetic, participând la o serie de activități de cercetare în Europa, Republica Populară Chineză și Statele Unite ale Americii. Prima activitate de cercetare a subiectului ales s-a materializat în luna iulie a anului 2016, când a participat Școala de vară „*Sino-EU Doctoral Summer School: For Logistics, Information, Management, and Service Science*", organizată în Beijing, Republica Populară Chineză, sub cupola Universității Jiaotong din Beijing, unde a susținut un seminar în aria curriculară a securității cibernetice, ocazie cu care a conferențiat pe marginea domeniului managementului securității cibernetice și a susținut plenar o lucrare cu titlul „*Global Internet Governance - International actors and the global cybersecurity dilemma*". În acest context, directorul[1] Departamentului de Managementul Informației și Sistemelor Informaționale din cadrul Universității Jiaotong din Beijing a venit în ajutorul autorului în procesul de documentare și identificare a resurselor necesare pentru construirea unui punct de vedere obiectiv asupra managementului

1. prof. univ. dr. Shifeng Liu, directorul Departmentului de Managementul Informației și Sistemelor Informaționale din cadrul Universității Jiaotong din Beijing, profesor în cadrul Facultății de Științe Economice și Management din cadrul Universității Jiaotong din Beijing, *http://en.sem.bjtu.edu.cn/faculty/ft/9248.htm.*

sistemelor informaționale și a conceptualizării din prisma teoriei ecologiei rețelelor[1].

Pentru a verifica teoriile, ipotezele și cazuistica colectată, în luna iulie a anului 2017, autorul s-a deplasat în Las Vegas, statul Nevada, Statele Unite ale Americii, la unul dintre cele mai ample evenimente din domeniul securității cibernetice din lume la acea dată[2], unde un număr de aproximativ 25.000 de practicieni înregistrați au avut ocazia să-și testeze teoriile și să-și demonstreze experimental practicile, atât în laboratoare de testare, cât și în cadrul sesiunilor de lucru. Acest eveniment a fost unul dintre elementele decisive pentru munca de documentare și cercetare, deoarece, cu ajutorul experienței acumulate pe parcursul șederii, autorul a reușit să testeze funcționalitatea unor sisteme de management ale securității informației în mediile virtuale și să infirme o serie de informații colectate.

Procesul de documentare continuă pe întreaga perioadă a elaborării tezei de doctorat i-a permis autorului să observe, în contextul guvernanței securității cibernetice, dinamica schimbărilor de ordin politic, tehnic și legislativ.

Pentru a putea trata subiectul securității naționale în contextul prezentei teme de cercetare, este obligatorie delimitarea securității cibernetice de celelalte arii de studiu și cercetare a securității. În această ordine de idei, este oportun ca în introducerea tezei să demistificăm incidența securității cibernetice ca ramură a studiilor de securitate în contextul curentelor şi școlilor de gândire. Totodată, este necesar studiul și evaluarea impactului securității cibernetice asupra dezvoltării și capacitării sectorului securității naționale în raport cu noile riscuri și amenințări apărute o dată cu evoluția tehnologică din domeniul comunicațiilor și tehnologiei informației. Este pe de-o

1. Mark Lubell, „Governing Institutional Complexity: The Ecology of Games Framework", în *The Policy Studies Journal*, Vol. 41, Nr. 3, 2013, pp.537-559, https://doi.org/10.1111/psj.12028, accesat în data de 21.06.2016.
2. DEF CON 25, 27-30 iulie 2017, https://www.defcon.org/html/defcon-25/dc-25-index.html, accesat în data de 04.08.2017.

parte evident, iar pe de altă parte recunoscut faptul că sistemul internațional - de apărare, comunicații, informații șamd- este supus unui amplu proces de transformare digitală radicală. Immanuel Wallerstein[1], John W. Meyer[2] şi Albert J. Bergesen[3] au evidențiat în mai multe rânduri importanța fuziunii dintre analiza puterii şi bunăstării și analiza aspectelor culturale şi cea a elementelor de suveranitate ale statului. *Cu toate acestea, doar o parte a politologilor au căzut de acord cu privire la faptul că sfârșitul Războiului Rece a confirmat teoria mai sus menționată, înlocuind frica declanșării unui război sau conflict nuclear, iar marile puteri sunt cele care domină sursele generatoare de securitate. Aceste surse generatoare de insecuritate erau reprezentative prin posibilul grad de risc, dimensiunea pericolelor şi forma amenințărilor directe la adresa securității naționale şi internaționale - uneori chiar globale. Printre acestea se numără: conflictele interetnice, dificilul proces de tranziție economică în statele fostului bloc comunist, creșterea fenomenului migraționist, creșterea nevoii și impactului indus de apartenența culturală şi religioasă, atât în sectorul societal, cât și în relațiile internaționale, nevoia de restructurare europeană şi importanța integrării euroatlantice a statelor din centrul și estul Europei. Aceste tendințe mai sus enunțate sunt doar o parte dintre cele care au generat necesitatea de a extinde şi aprofunda semnificația și definiția conceptului de securitate*[4].

Dilemele securității şi conflictelor au fost câteva din preocupările celor mai de vază gânditori ai antichității, precum Aristotel, Platon, Cicero, Xenofon, care au făcut referiri în scrierile lor la problematica păcii şi a conflictelor, respectiv a războiului, a consecințelor acestora și desigur a impactului acestora asupra progresului națiunii.

---

1. Immanuel Wallerstein, https://iwallerstein.com/, accesat în data de 08.08.2020.
2. John W. Meyer, https://sociology.stanford.edu/people/john-meyer, accesat în data de 08.08.2020.
3. Albert J. Bergesen, https://arizona.pure.elsevier.com/en/persons/albert-j-bergesen, accesat în data de 08.08.2020.
4. Alexandra Sarcinschi, *Elemente noi în studiul securităţii naţionale şi internaţionale*, Editura Universităţii Naţionale de Apărare, Bucureşti, 2005, pp.7-8.

Pe parcursul anilor, în contextul abordării din partea statelor a diferitelor domenii de cercetare - *securitate umană, militară, politică, a mediului, economică, spațială, cibernetică șamd* - au fost organizate summit-uri, întâlniri de lucru instituționale și dezbateri științifice pe tema securității și a subdimensiunilor acesteia. Un aspect este cert, conceptul de securitate își păstrează în continuare caracterul ambiguu și dinamic. Conceptul de securitate în *procesul de cercetare al relațiilor internaționale* este utilizat adesea ca pretext, scuză ori justificare pentru atingerea diverselor obiective sau rezultate adesea strategice în raport cu statele partenere și nu numai. Definitoriu, termenul de „*securitate națională*" are un caracter amorf, acesta suferă adesea reinterpretări legislative actualizate anual sau la o frecvență de cinci ani - aici făcându-se referire directă la strategiile naționale ori sectoriale în domeniul apărării, securității naționale, a planurilor de priorități emise de C.S.A.T. sau C.N.I.[1]

Într-un mod natural, fiecare școală și curent de gândire au definit într-un mod diferit securitatea, fiecare dintre acestea lăsând o amprentă aparte izvorâtă din curentul filosofic îmbrățișat. Cu toate acestea, nici una dintre școlile de gândire nu și-a permis asumarea unei definiții absolute și complete în limita rigorii științifice. În accepțiunea actuală - după încheierea Războiului Rece - definitoriu, noțiunea de securitate aparține gândirii îmbrățișate de Școala de la Copenhaga (1980/1985-1988). În aceeași ordine de idei, se pot enunța câțiva dintre cercetătorii consacrați în domeniul securității, precum Ole Wæver[2], Barry Gordon Buzan[3], Jacobus Hubertus „*Jaap*" de Wil-

1. Cristian Niță, „Securitatea Naţională – O Perspectivă Academică", p.3, http://www.nos.iem.ro/bitstream/handle/123456789/33/4.1.Sec%20Academic%20nita.pdf?sequence=1&isAllowed=y, accesat în data de 30.07.2019.
2. Ole Wæver, https://politicalscience.ku.dk/staff/Academic_staff/?pure=en%2Fpersons%2Fole-waever(616ba573-b094-46ed-a29b-56d8f2a5049e)%2Fcv.html, accesat în data de 08.08.2020.
3. Barry G. Buzan, https://www.lse.ac.uk/international-relations/people/buzan, accesat în data de 08.08.2020.

de[1], Jef Huysmans[2], a căror opere sunt adesea considerate pietre de temelie în cercetarea oricărui subdomeniu al securității, unul dintre acestea fiind securitatea cibernetică.

„Situată între abordările clasice (realism vs liberalism) şi studiile pentru pace (vezi operele unui Kenneth Boulding, John Burton sau cele ale lui Johan Galtung din cadrul institutului Transcend), Școala/paradigma Copenhaga înțelege securitatea ca pe un evantai de nuanţe intermediare între război şi pace."[3] În acest context, Școala de la Copenhaga influențează modalitatea de conceptualizare a definiției securității pe o structură de cinci niveluri generale, respectiv: militar, economic, politic, de mediu și social.

Definițiile securității sunt emise de autori consacrați în studiul și cercetarea securității - precum Ian Bellany care definește "*securitatea în sine ca o relativă absenţă a războiului, combinată cu o relativ solidă convingere că nici un război care ar putea avea loc nu s-ar termina cu o înfrângere*", Walter Lippman care emite prezumția că "*o naţiune este în siguranţă în măsura în care nu se află în pericolul de a trebui să-şi sacrifice valorile fundamentale, dacă doreşte să evite războiul, şi poate, atunci când este provocată, să şi le menţină obţinând victoria în război*"[4], sau Mroz J. Edwin care definește „*securitatea ca fiind absența relativă a amenințărilor cu distrugerea*"[5].

Pe de altă parte, instituții de profil în domeniul securității emit definiții asupra securității izvorâte din aria de expertiză, din interesul instituțional legitim și poziționarea statelor deservite în raport

1. Jacobus Hubertus „*Jaap*" de Wilde, https://www.rug.nl/staff/j.h.de.wilde/cv, accesat în data de 08.08.2020.
2. Jef Huysmans, https://www.qmul.ac.uk/politics/staff/profiles/huysmansjef.html, accesat în data de 08.08.2020.
3. Georgeta Chirlesan, *Strategia de securitate naţională a României: evoluţii şi tendinţe între securitatea regională şi cea euro-atlantică*, Editura Academiei Forțelor Terestre „Nicolae Balcescu", Sibiu, 2013, pp.34-35.
4. Barry Buzan, *Popoarele, statele şi teama. O agendă pentru studii de securitate internaţională în epoca de după Războiul Rece*, Ed. Cartier, Chișinău, 2000, p.28.
5. John Edwin Mroz, *Beyond Security, Private Perceptions Between Arabs and Isrealis*, Ed. International Peace Academy, New York, 1991.

cu întreg conceptul de „*securitate*". Un concept interesant și simplist care a fost remarcat este cel al *National Defence College (Canada)*, care descrie securitatea ca fiind acțiunea de susținere și păstrare a unui mod de viaţă stabil pentru popor și stat, în echilibru și conform nevoilor şi aspiraţiilor de drept ale celorlalți. În viziunea acestuia, securitatea include omiterea sau aplanarea conflictelor armate şi desigur a coerciției, o stare de stabilitate și limitare a posibilității de subminare *a status quo-ului* intern, precum şi eliminarea factorilor de eroziune a valorilor politice adoptate, a celor economice, respectiv sociale, care sunt absolut esențiale păstrării unui bun nivel de calitate a vieţii în societate[1].

În ceea ce privește definiția securității naționale, formula dezvoltată de Penelope Hartland Thunberg poate fi considerată etalon, aceasta prezentând „*securitatea naţională ca reprezentare a capacității unei națiuni de a-şi urmări cu succes interesele naționale, așa cum le concepe ea oriunde în lume*"[2]. Pornind de la aceasta, Ole Wæver extinde definiția, considerând „*securitatea drept un act de vorbire unde afirmarea în esența sa constituie actul de securizare. Termenul „securitate" expus de o elită națională reorientează definitoriu actul de securizare dinspre particular spre specific, context în care se poate pretinde un drept special de a folosi întreg instrumentarul în virtutea nevoii de a bloca această evoluție (de insecuritate)*"[3] În egală măsură, Arnold Wolfers concepe „securitatea, în sens obiectiv, măsoară absenţa ameninţărilor la adresa valorilor dobândite, iar într-un sens subiectiv, absenţa temerii că asemenea valori vor fi atacate"[4].

1. Martin Griffiths, *Relaţii internaţionale. Şcoli, curente, gânditori*, (trad. Cristea Darie, Popistaşu Olga, Barna Cristian), Editura Ziua, Bucureşti, 2003, pp. 167-182.
2. Penelope Hartland-Thunberg, „National Economic Security: Interdependence and Vulnerability" în vol *National Economic Security: Perceptions, Threats, and Policies* (ed. Frans Alphons Maria Alting von Geusau, Jacques Pelkmans), Edit. John F. Kennedy Institute, Olanda, 1982, p.51.
3. Ole Wæver, „Securitization and Desecuritization', în vol. *On Security* (ed. Ronnie D. Lipschutz), Edit. Columbia University Press, New York, 1995, pp. 46-86.
4. Arnold Wolfers, „National Security as an Ambiguous Symbol", în *Political Science Quarterly*, Vol.67, Nr. 4, Edit. Academy of Political Science, New York, 1952, pp. 481-502.

În România, prin hotărârea C.S.A.T., s-a validat o doctrină națională[1] și mai reprezentativ prin SNAP, unde conceptul de *„securitate naţională”* este definit ca *„starea națiunii, a comunităților sociale, a cetățenilor şi a statului, fundamentată pe prosperitate economică, legalitate, echilibru şi stabilitate socio-politică, exprimată prin ordinea de drept şi asigurată prin acțiuni de natură economică, politică, socială, juridică, militară, informațională şi de altă natură, în scopul exercitării neîngrădite a drepturilor şi libertăţilor cetățenești, manifestarea deplină a libertății de decizie şi de acțiune a statului, a atributelor sale fundamentale şi a calității de subiect de drept internațional.”* Prin Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024 se *„propune un management al problematicii de securitate naţională cu accent pe gestionarea integrată a riscurilor, amenințărilor şi vulnerabilităților de către statul român”* într-o dublă valență, pe de-o parte *„internă, naţională, în spiritul edificării unei autentice comunități de securitate, apărare și ordine publică”*, iar pe de altă parte *„cea europeană, euro-atlantică şi internațională, România asumându-și responsabilitățile ce-i revin în calitate de membru al UE, NATO, OSCE, ONU şi al altor organizații internaționale”*[2]

Definiția securității naționale mai sus definită prin doctrină și SNAP este una generală, dar care evidențiază liniile principale de acțiune ale României în vederea asigurării unui mediu de securitate optim, conform nevoilor de securitate ale cetățeanului și ale valorilor țării.

Algoritmul praxiologic ar putea fi argumentat prin ecuația *„starea **referentului** x fundamentată pe **valorile** y, asigurată prin **mijloacele** z, în **scopurile** w”*, unde **referentul** x este reprezentat de însăși națiune, alocându-i-se de drept calitatea de subiect și beneficiar de securitate

1. „Doctrina naţională a informaţiilor pentru securitate”, adoptată de C.S.A.T. în 23 iunie 2004, http://arhiva.sri.ro/doctrina-nationala-a-informatiilor-pentru-securitate.html, accesat în data de 11.08.2020.
2. Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024, p.7, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accesat în data de 11.08.2020.

în comunități, societate şi desigur stat. Fundamentarea acestuia pe **valori** reprezentate de factori ca stabilitatea socio-politică, prosperitatea economică generală, contextul legitim și echilibrul puterilor în stat reprezintă motivația în alegerea **mijloacelor** optime de asigurare a unei stări de normalitate reflectate adesea în multitudinea acțiunilor de natură politică, economică, socio-culturală, juridică, informațională, militară șamd. **Scopurile** sau obiectivele sunt adesea date de posibilitatea de manifestare deplină a capacității și libertății de decizie şi acțiune a statului, precum şi a calității acestuia de subiect de drept internațional.[1]

Observăm așadar conceptul de securitate general, care are un caracter aparent amorf, prin care în actualul context de securitate se pot identifica nevoia și posibilitatea de definire a conceptului de securitate cibernetică.

Apariția arealului cibernetic duce la lărgirea contextului de securitate și insecuritate adus de conflictele globale[2] deja existente în sectorul social, politic și militar internațional. Înarmarea cibernetică a statelor chiar înainte de STUXNET, cum este cazul SUA sau Israel în raport cu acțiunile altor state ca Iran[3] sau Coreea de Nord[4], crește exponențial riscurile trecerii de la stadiul de conflict la stadiul de război. Limitarea conceptuală a definiției conceptului de *„securitate"* la cea de *„securitate națională"* și *„securitate supranațională"* este de cele mai multe ori motivată de nevoia asigurării unei integrități teritoriale în interes național. Unul dintre rezultatele unei astfel de

1. Cristian Niță, *op.cit.*, p.4.
2. *Tensiuni diplomatice care au escaladat între SUA, Israel și Iran, Golful Persic sau Coreea de Nord.*
3. Zolan Kanno-Youngs, Nicole Perlroth, „Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat Grows", 08.01.2020, https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html, accesat în data de 11.08.2020.
4. Departamentul de Stat al SUA, Trezoreria SUA, Departamentul de Securitate Internă a SUA, FBI, DPRK Cyber Threat Advisory, „Guidance on the North Korean Cyber Threat", 15.04.2020, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_cyber_threat_advisory_20200415.pdf, accesat în data de 11.08.2020.

limitări sau interpretări duce la excluderea amenințărilor din algoritmul fundamental al definiției. Conceptul de securitate acoperă toate subdomeniile a căror arie de interes relaționează cu definiția generală a acestuia. Limitarea conceptuală a securității la anumite subdomenii aduce un deserviciu procesului de dezvoltare a securității naționale în plan intern sau extern și în mediul național sau internațional.

Reconceptualizarea definitorie a securității în maniera includerii în aceasta şi a dimensiunii cibernetice, unde „securitate *cibernetică*" să reprezinte o subdimensiune a „*securității*", este absolut necesară. Securitatea cibernetică reprezintă o realitate a preocupării generale de a identifica şi alte dimensiuni ale viitoarei agende de securitate (*factori militari, economici, politici, culturali, de mediu șamd*).

Puternic motivate de nevoia de securitate în plan regional și uneori în virtutea mândriei naționale, a suveranității și a siguranței naționale, statele mai puțin reprezentative în contextul geopolitic și de securitate global își pun teritoriile la dispoziția[1] statelor dominante în context politic, economic și militar sau a puterilor supranaționale. Dacă înarmarea nucleară a devenit un element care oferă statelor dominante un avantaj care transcende însuși conceptul de suveranitate națională, atunci conceptul securității cibernetice în domeniul securității naționale poate deveni un atu la îndemâna oricărui stat care deține informația vitală, resursa tehnică și umană necesară dezvoltării de sisteme generatoare de securitate sau insecuritate.[2] Acțiunile ofensive și defensive din ultimii ani au dovedit că orice stat poate deveni o putere în plan cibernetic, fie că este sau nu un stat dominant în context regional sau global.

Pe parcursul documentării și chiar înaintea aplicării chestionarelor, s-a ridicat întrebarea dacă evaluarea nivelului de securitate ciber-

1. Arnold Wolfers, *Discord and Collaboration: Essay on International Politics*, Edit. The Johns Hopkins Press, Baltimore, Maryland, SUA, 1962, p.192.
2. Mathew Ha, David Maxwell, *Kim Jong Un's ‚All-Purpose Sword' North Korean Cyber-Enabled Economic Warfare*, Edit. FDD PRESS, Washington, DC, SUA, 2018, p.6.

netică a populației reflectă sau influențează într-o oarecare măsură integritatea securității naționale. La baza proiectării unui sistem de securitate cibernetică competitiv și a consolidării spațiul cibernetic se regăsește prezumția de nevinovăție acordată tuturor utilizatorilor și gradul de încredere crescut asupra utilizării resurselor digitale de către aceștia. Bazat pe acest principiu, resursele internetului spre exemplu pot fi exploatate în acest moment, conform raportului statistic al Miniwatts Marketing Group, de către cei peste 4,833,521,806 de utilizatori din totalul populației lumii de 7,796,949,710[1] în data de 12.08.2020. Așadar, conform statisticilor efectuate asupra folosirii resurselor digitale de către utilizatorii sistemelor informaționale contemporane, putem spune că gradul de utilizare al spațiului cibernetic și al resurselor vehiculate prin acesta este foarte mare. Întreg arealul cibernetic cu resursele, beneficiile și oportunitățile aduse de acesta este parte componentă a vieții cetățenilor din țările civilizate. Dacă ne raportăm la Estonia, în anul 2020, această țară oferea aproximativ 2600 servicii online, printre care se numără reînnoirea permisului de vânătoare sau posibilitatea de a vota de la distanță doar cu buletinul digital.[2] Raportat la numărul atacurilor cibernetice și la complexitatea acestora, se poate considera că dinamica și gradul de „*conectare*” online al unei comunități sau națiuni cresc în mod absolut gradul de risc și nivelul de vulnerabilitate al utilizatorilor conectați. În acest context, observăm că nu există o țară care să fie protejată de expunerea la acțiuni de vulnerabilizare și riscuri generate de alte state, de grupări izolate sau activiști puternic motivați în mediul virtual - motivați politic, social, financiar, ideologic, religios sau pur și simplu rău intenționați. În România ultimilor ani s-au evidențiat atacuri cibernetice desfășurate într-o formă crescută de agresivitate,

1. Internet World Stats, „*World internet usage and population statistics*”, iunie 2019 https://www.internetworldstats.com/stats.htm, accesat în data de 29.07.2019.
2. Cristina Cileacu, „Estonia, avansată în era digitalizării”, în emisiunea *Pașaport diplomatic*, 29.05.2020, https://www.youtube.com/watch?v=cFMyF1__WNA, accesat în data de 12.08.2020.

aici putem oferi exemplu Red October, MiniDuke sau cel facilitat de Wipbot/Epic. Nenumărate atacuri apar în ultimii ani în presă și pe canalele de mass-media, dar cele mai importante, care pot aduce sau au adus atingere securității naționale, sunt în continuare necunoscute publicului larg. Atacuri de tipul (spear)phishing, DDoS (și derivate ale acestui tip de atac), APT și multe altele vizează și instituții de stat. Principalele obiective ale acestor atacuri sunt de obținere a accesului la sistemele, terminalele, echipamentele și rețele informatice de interes național, precum și exfiltrarea de date nesecrete, nedestinate publicității sau secrete de serviciu. Este evident acum faptul că conceptul *„securității cibernetice"* reprezintă o subdimensiune a securității naționale asupra căreia guvernele își concentrează atenția, emițând în ultimii ani actualizări ale legislației naționale, legi speciale și metodologii de aplicare a acestora. Revine statului întreaga responsabilitate privind gestionarea arealului cibernetic și a adoptării de măsuri în vederea respectării dreptului constituțional al cetățeanului, a integrității și suveranității statului, respectiv a securității naționale.

Guvernanța spațiului cibernetic se lovește printre altele și de provocări în plan legislativ și judiciar, prin permanentele campanii ofensive aduse la adresa întregii populații, precum și la adresa instituțiilor publice. Acesta este recunoscut ca fiind fenomenul tranziției actului infracțional și criminal din arealul fizic în cel virtual. În acest context, caracterul dinamic al acestui fenomen și capacitatea de a influența într-un mod eficient modul de manifestare al amenințărilor tradiționale, aduc adesea în prim plan nevoia de conștientizare, de prevenire și contracarare, dar și de creștere a culturii de securitate în plan tehnologic, organizațional și desigur legal.[1]

În context internațional, european, noțiunea „*securitate națională*", menționată în art.8, art.10 și art.11 din „*Convenția Europeană pentru*

1. Florian Coldea, Intelligence, „Securitatea cibernetică, de la „perla coroanei" în IT spre „business as usual" în societate", https://intelligence.sri.ro/securitatea-cibernetica-de-la-perla-coroanei-spre-business-usual-societate/, accesat în data de 29.07.2019.

Apărarea Drepturilor Omului și a Libertăților Fundamentale", este definită lacunar, drept urmare jurisprudența CEDO a delimitat contururile acesteia. În concluziile Raportului se recunoaște puterea discreționară a statelor privind evaluarea amenințărilor la adresa securității naționale și a alegerii mijloacelor de contracarare și combatere. Chiar și așa, statele sunt nevoite să trateze cu maximă responsabilitate amenințările și acțiunile luate împotriva acestora, existând de altfel și necesitatea aplicării principiului măsurii rezonabile, *„cu mențiunea faptului că Marja de apreciere a statului în cauze legate de securitatea națională nu mai este uniform de largă. În anumite cazuri, orice marjă de apreciere este exclusă în mod explicit prin însăși natura art. 3."*[1] Drept urmare, Curtea s-a pronunțat prin reducerea marjei de apreciere în anumite domenii, unul dintre acestea fiind libertatea de exprimare în timpul serviciului militar sau în timpul liber și privat al cadrelor militare.

În ceea ce privește acțiunile instituțiilor de profil din România, se poate evidenția impactul avut de recunoașterea acestei noi dimensiuni a securității și chiar redefinirea securității cibernetice de către Serviciul Român de Informații, care, în urma atacurilor cibernetice cu motivație strategică asupra infrastructurilor guvernamentale IT&C din alte state în 2008, a răspuns prin reconceptualizarea sistemelor proprii și asigurarea securității cibernetice a infrastructurilor IT&C cu valențe critice existente la nivel național. SRI a înființat două departamente cu atribuții în acest sens. Este vorba de un departament care a abordat securitatea cibernetică din perspectiva HUMINT și un departament care a realizat abordarea din perspectivă tehnică.

În anul 2013, s-a materializat prima *Strategie de securitate cibernetică*[2], act care marchează, conceptual și definitoriu *„securitatea ciber-*

1. Curtea Europeană a Drepturilor Omului, Divizia Cercetare, CE, „Securitatea națională și jurisprudența Curții Europene a Drepturilor Omului", http://ier.gov.ro/wp-content/uploads/2019/06/RC-Securitatea-nationala-si-jurisprudenta-CEDO-2013.pdf, p.39.
2. Hotărârea de Guvern nr. 271 din 25.03.2013 *pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea*

netică" în România, urmată de Hotărârea C.S.A.T., care desemnează S.R.I. ca autoritate națională de *cyberintelligence*. Drept urmare, S.R.I. își concentrează atenția pe înființarea unei unități specializate în prevenirea și contracararea amenințărilor cibernetice existente la adresa tuturor infrastructurilor critice IT&C care au capacitatea de a afecta sistemele de securitate națională, numit Centrul Național CYBERINT.

Începând cu anul 2014, interesele NATO și UE privitoare la creșterea nivelului de securitate cibernetică au fost tot mai mari și specifice.[1] România depune în continuare eforturi considerabile pentru consolidarea securității naționale din perspectiva securității cibernetice, fie împreună cu UE și NATO în context de securitate național, internațional și mondial, folosindu-se de toate relațiile de cooperare, alianțele și parteneriatele încheiate. Motivația este, desigur, iminenta „*integrare globală economică, socială și teritorială generată de industria comunicațiilor*"[2], cooperarea internațională, schimbul de bune practici în materie de cercetare, inovație tehnologică și interoperabilitate a sistemelor, reconceptualizarea securității cibernetice și adoptarea unui cadru de reglementare adecvat.

Sistemului național de securitate cibernetică.

1. Anton Rog, Cristian Condruț, „Evoluția amenințării cibernetice", în *Intelligence în serviciul tău*, nr.38, Edit. SRI, București, 2019, pp.10-11.
2. Robert Lupitu, „Ministrul Comunicațiilor, vizită în SUA. Alexandru Petrescu s-a întâlnit cu consilierul lui Donald Trump pentru politica de securitate cibernetică a Statelor Unite", https://www.caleaeuropeana.ro/ministrul-comunicatiilor-vizita-in-sua-alexandru-petrescu-s-a-intalnit-cu-consilierul-lui-donald-trump-pentru-politica-de-securitate-cibernetica-a-statelor-unite, accesat în data de 07.08.2019.

Capitolul II. Managementul informațiilor electronice vehiculate în mediul virtual

În cadrul cercetării, *managementul informației* este rezultatul gestionării raportului între *planificare - colectare - procesare - analiza și sinteza - valorificarea* acesteia pentru o livrare către factorul de decizie și utilizarea acesteia într-un mod eficient. Ținând cont de faptul că gradul de performanță al guvernanței unui mediu, chiar și al celui virtual, se raportează la calitatea, veridicitatea și momentul livrării informației, putem spune că în centrul guvernanței sistemelor informaționale și a întregului areal cibernetic stă informația.

Cu alte cuvinte, managementul informației pornește de la planificarea modalităților de lucru și trasarea unor limite de timp și resurse, în același timp se stabilesc direcțiile de acțiune a celor angrenați în procesul de colectare a datelor și informațiilor. Următorii pași sunt făcuți în direcția procesării informației colectate în vederea utilizării

acesteia ca material relevant în conținutul rapoartelor de analiză, etapă în care datele - *în toate formele sale* - și informațiile sunt verificate și utilizate în vederea obținerii unor prognoze asupra impactului dat de existența acestora și furnizarea de răspunsuri la principalele cerințe solicitate de beneficiarul sistemului de management al informației. Diseminarea rezultatelor proceselor mobilizate în cadrul sistemului de management al informației este un răspuns la solicitarea beneficiarului de drept, ca urmare raportul final îi revine acestuia. În urma diseminării, un ultim pas este cel de furnizare sau solicitare a unui punct de vedere din partea beneficiarului asupra funcționalității proceselor mobilizate în sistemul de management al informației, indirect asupra metodelor, tehnicilor, resurselor și desigur persoanelor care și-au adus aportul în atingerea obiectivelor propuse.

Fie că vorbim de sectorul militar, cel de guvernământ sau de cel civil, indiferent în ce scop este utilizată, informația preia un atribut atât tactic cât și operațional[1] considerabil.

Informația, în orice formă s-ar afla, trebuie identificată, observată, extrasă, analizată și prelucrată pentru a-i putea atribui o valoare în vederea folosirii acesteia. De aceea, relevanța managementului informațiilor din mediile electronice, în contextul domeniului de analiză al studiilor de securitate, este una vitală atât pentru beneficiar, cât și pentru decidenții corporativi, industriali, guvernamentali, politici, diplomați, înalți guvernanți, sau pentru orice actor statal sau non statal ale căror decizii se învârt în jurul acestor informații[2].

Nevoia unui sistem informațional bine structurat se face simțită în cadrul organizațiilor unde informația este nu doar sensibilă, ci atributul său dinamic face ca o informație care nu se află în format

1. Aurelia Peru-Balan, Vitalina Bahneanu, „Războiul informațional, Propaganda, Fake-News: Controlul asupra percepției publice", în *MOLDOSCOPIE*, Nr. 1, Vol. LXXX, Chișinău, 2018, pp.129-131.
2. Teodor Frunzeti, Cristian Bărbulescu, „Reziliența națională la amenințările hibride și cultura de securitate. Un cadru de analiză", p.4, http://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf, accesat în data de 23.07.2019.

electronic să fie mult mai greu de multiplicat, gestionat sau arhivat; pe de altă parte alterarea acesteia este oricum inevitabilă, pe când un document în format electronic (*text, audio, video, radio*), gestionat conform normelor minime de securitate, nu este la fel de vulnerabil la aceste riscuri. Cu toate acestea, trebuie menționat că volumul informației crește exponențial cu progresul tehnologic, creșterea populației și a surselor generatoare de informații, drept urmare informația în acest moment poate fi generată de mult mai multe surse, în multe alte formate decât în trecut și poate fi propagată printr-o multitudine de canale de comunicații. Acesta este motivul principal pentru care trebuie să acordăm o atenție sporită verificării informației, identificând mereu sursa de proveniență și analizând mereu aspectele de formă sau conținut.

În acest context, în era globalizării informației, caracterizată de ritmul alarmant de generare, multiplicare și repudiere a datelor și informațiilor, de creștere a gradului de disponibilitate și accesibilitate a acestora, s-a impus în majoritatea statelor din spațiul euroatlantic reevaluarea paradigmei de securitate a datelor vehiculate prin surse deschise și prin cele clasificate. Spre exemplu, la nivel statal de această dată, una dintre schimbările care au avut loc a fost cea de reevaluare a paradigmei tradiționale a proceselor de intelligence, cu un impact major adus ariei de conceptualizare a activităților, din perspectivă conceptuală, metodologică și organizatorică. Această schimbare a fost determinată de acțiunea unor factori de natură exogenă[1] și endogenă[2] [3].

1. Factori exogeni: *proliferarea surselor de conflict și a actorilor, caracterul transnațional al riscurilor, factorii de risc și oportunitate ai evoluției tehnologice cu impact în activitățile de intelligence, apariția și extinderea unor noi forme de conflict neconvențional șamd.*
2. Factori endogeni: *dinamica legislativă ori strategică națională, impact financiar, recapacitarea capitalului uman, modificarea culturii organizaționale, revizuirea și adaptarea metodelor și procedurilor standard, șamd*.
3. Ionel Nițu, „Analiza de Intelligence, O abordare din perspectiva teoriilor schimbării", Edit. Rao, București, 2012, pp.67-72.

Întrebările din ale căror răspunsuri vor rezulta eventuale soluții la situațiile stringente ale sistemului organizațional contemporan în ceea ce privește managementul informației sunt următoarele:

- *Ce reprezintă din punct de vedere informațional organizația?*
- *Care sunt, din perspectiva managementului riscului, vulnerabilitățile, variabilele de risc și implicațiile la care sunt supuse sistemele informaționale asupra și în cadrul organizației?*
- *Putem vorbi despre nevoia unei reorganizări de securitate și management al informației într-o organizație?*

Odată cu evoluția tehnologică, a progresat și știința informației. Știința informației s-a dezvoltat treptat pe patru perioade mari de timp. Înainte de anul 1600 știința informației se regăsește într-o perioadă de descoperire și identificare a potențialelor arii și direcții de dezvoltare. În intervalul 1600-1950 aveam de-a face cu o știință a informației teoretică, fără rezultate notabile în ceea ce privește procesarea informației sau analiza acesteia la scară largă. Ceva mai recent, modelele teoretice au motivat experimentele și cercetarea potențialului informației prelucrate. În mod natural, în intervalul 1950-1990, am început să experimentăm știința asistată de calculator sau știința comunicațiilor și tehnologiei informației. Fiecare ramură științifică a dobândit și o ramură computațională. Asistarea calculatorului în diferite domenii a oferit noi soluții, anume modelele matematice complexe, ceea ce a făcut ca din 1990 până în prezent să experimentăm știința datelor informatice sau știința informației. Aceste științe sunt alimentate cu date și susținute de instrumente complexe de achiziție, măsurare și simulare în mediul online sau offline. Sunt utilizate serviciile de internet sau intranet și instrumentarul tehnologic modern eficient în identificarea, colectarea, gestionarea, analiza datelor din diverse surse pentru a oferi o înțelegere absolută a acestor date colectate și relaționarea dintre acestea pentru o perspectivă semnificantă în progresul general al organizației, tehnologii

numite data „*warehousing*”[1] și „*data mining*[2]”. Chiar dacă nu folosim individual pe dispozitivele noastre de comunicații volume mari de date, trebuie să ținem cont că toate aceste informații, trecând prin sistemele de comunicații sau doar stocate și procesate în soluții de tip „*cloud*”[3] sau în diverse baze de date, pot să ajungă la volume impresionante pe care sistemele informaționale sunt nevoite să le acceseze, volume care au ajuns de la dimensiunea de 1 Byte, care poate fi exemplificat prin capacitatea purtată de un caracter precum litera „*a*”, la 1 Yottabyte (YB), care poate fi reprezentat printr-un număr de 257.054.773.251.740 discuri DVD, fiecare cu capacitatea de 4.38 GB. Cu toate că deținem atât de multă informație la un click distanță, nu este suficient, deoarece ne pierdem în acest tumult de date nestructurate și totuși suntem în același timp însetați de cunoaștere.

II.1. Organizația sursă generatoare de securitate a informației

Etimologic, cuvântul organizație derivă din limba greacă, de la termenul *ὄργανον*, care are sensul de instrument, unealtă, provenit la rândul său din forma proto-indo-europeană **werǵ*- (“muncă”). Organizația poate fi definită o dată ca o asociație de capital social cu preocupări comune care a consimțit să acționeze în vederea atingerii unui scop comun. Organizația se referă și la modul de organizare sau aranjare a elementelor - *ideologice, juridice, materiale, financiare, umane*

1. Ronald van Loon, *What Is the Future of Data Warehousing?*, 18.09.2016, https://mapr.com/blog/what-future-data-warehousing/, accesat în data de 12.05.2018.
2. Bhavani M. Thuraisingham, Latifur Khan, Mehedy Masud, Kevin W. Hamlen, „Data Mining for Security Applications”, în *Proceedings 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008* https://www.researchgate.net/publication/221452043_Data_Mining_for_Security_Applications, accesat în data de 02.05.2019.
3. Lori M. Cameron, „What is cloud computing? Seven years later, has the time come to officially redefine it?”, 24.07.2018,https://publications.computer.org/cloud-computing/2018/07/24/cloud-computing-definition-nist/, accesat în data de 26.07.2018.

- care o definesc în vederea desfășurării proceselor cu maximum de eficiență și reziliență[1].

O dată cunoscute aceste aspecte, putem analiza organizația din punct de vedere informațional ca fiind un întreg de procese interconectate și dependente unele de altele, procese precum creșterea ponderii informației în organizație și societate, a vehiculării acesteia în cadrul organizației, rolul și importanța informației în contextul dezvoltării organizaționale, cu accentul pe necesitatea protejării ei ca o componentă a mediului organizațional de securitate.

Organizația reprezintă o entitate dominantă în toate sectoarele societății, ca formă prin care acțiunea colectivă este combinată cu abilitățile individuale agregate, pentru realizarea majorității categoriilor de bunuri economice[2]. În lipsa unui consens privind definiția generală a conceptului de *„organizație"*, majoritatea autorilor preferă să menționeze semnificații ale conceptului sau o listă de caracteristici ce poate fi utilizată în loc de definiție, o mențiune sau notă descriptivă cu scop operațional, care este necesară pentru o abordare pragmatică, așa cum este cea a managementului. Astfel pusă problema definiției, se poate afirma că *„o organizație este un grup de oameni care acționează într-un mod corelat pentru atingerea unui scop comun"*. Definiții similare în esență, dar mai sofisticate în privința exprimării oferă și alți teoreticieni din economie, sociologie, psihologie și alte științe ce operează cu acest concept[3]. Actualmente, conceptul "*organizația*" constă într-o varietate de forme înfățișate sub structura organizatorică a unui partid politic, a unei întreprinderi economice, primării, a ministerelor și agențiilor ofertante de servicii, organizații religioase şi stații radio-TV, magazine, restaurante, piețe şi multe alte-

1. Academia Română, Institutul de lingvistică "Iorgu Iordan", *Dicționarul Explicativ al Limbii Române*, Ediția a II-a, Edit. Univers Enciclopedic, București, 1998, p.727.
2. Vlăsceanu Mihaela, *Organizatii și comportament organizational,* Edit. Polirom, Iași, 2003.
3. Bogdan Băcanu, *Organizație publică – Teorie și management,* Edit. Polirom, Iași, 2008, p.19.

le în care se desfășoară activități culturale, economice, educaționale, religioase, sanitare, comerciale șamd. În contextul sustenabilității și guvernanței sistemului de management, ne regăsim într-un sector dinamic, sensibil la modificări. Contextual unele organizații apar, altele dispar, unele fuzionează, altele își diminuează ponderea, pe când altele cresc rapid, iar altele luptă să supraviețuiască. Totodată, noile mijloace de informare şi comunicare şi-au adus propria contribuție în generarea unor organizații, care funcționează în rețele care transcend granițele clasice stabilite în timp şi spațiu. Mai mult, au apărut organizațiile virtuale, care sunt constituite sub forma rețelelor de comunicare rapidă intermediată de noile tehnologii informatice. Dar chiar și așa, datorită surselor generatoare de diversitate, timpul de supraviețuire a unei organizații într-o formă, mărime și profil s-a redus considerabil, după unele estimări la 5-10 ani[1]. Organizația ca temă de dezbatere reprezintă un subiect vast. În acest capitol, doresc să ghidez atenția pe trei dintre aspectele definitorii organizației ca mediu informațional.

Importanța cunoașterii organizației în procesul de guvernare a securității spațiului virtual este una definitorie. Așa cum o infracțiune nu poate fi cercetată fără a se cunoaște toate părțile infracțiunii, nici managementul securității domeniului cibernetic nu poate fi tratat fără a se cunoaște în primul rând organizația, în calitate de subiect al acțiunilor întreprinse în acest areal și desigur, de a se cunoaște calitatea de țintă deținută de organizație în contextul eventualelor campanii ofensive desfășurate în spațiul cibernetic.

Acestea fiind cunoscute, se poate deschide subiectul analizei organizației în vederea identificării elementelor componente ale ecuației de soluționare a problematicii securității domeniului cibernetic în cadrul organizațional.

1. Mihaela Vlăsceanu, *Organizația: proiectare și schimbare – Introducere în comportamentul organizațional*, Edit. Comunicare.ro, București, 2005, pp.60-61.

II.1.1. Analiza organizației

Procesul de analiză a organizației reprezintă unul dintre pilonii care asigură o bună continuitate a proceselor organizaționale. În ciclul de viață al organizației sunt momente în care analiza anumitor aspecte este necesară. Dintre acestea, pot fi amintite cazurile de restructurare, momentul tranziției în cazul schimbărilor de ordin managerial, de dezechilibru între incapacitatea de atingere a obiectivelor, comunicare defectuoasă și de nenumărate ori lipsa capacității de adaptare la schimbările legislative, insecuritate (*economică, cibernetică, umană șamd*). Problematica ce urmează a fi tratată în urma obținerii unor rezultate din procesul de analiză organizațională este de fapt un răspuns la întrebările de ordin funcțional ale organizației. O astfel de întrebare poate apărea în cazul unei lipse de comunicare între sectorul de management și cel operațional. În scopul reorganizării, spre exemplu, poate apărea o întrebare în vederea identificării unei soluții de creștere a productivității prin adoptarea unor măsuri de ordin tehnic și informatic în detrimentul utilizării forței de muncă umane.

Utilitatea unei analize a informației, chiar și de rutină, poate aduce lămuriri cu privire la orice eveniment ori fenomen organizațional, precum: fenomenul „*turnoverului*", satisfacția şi loialitatea personalului față de organizație, productivitatea şi eficiența unei structuri sau substructuri a organizației, comunicare şi conducere, performanța în organizație şi calitatea factorului decizional/conducere.

Studiul și analiza organizațională pornește de la asumarea unei definiții a organizației, motiv pentru care consider că organizația este un sistem complex în care se armonizează interesele individuale cu cele ale grupurilor, factorii mediului interior și ai mediului exterior, stimulii și restricțiile, tehnologia și inovarea, cerințele normative și

inițiativele informale[1]. Sintetizând această definiție, ajungem la o afirmație de forma "*organizațiile sunt sisteme de organizare inventate în scopul realizării unor obiective prin efort comun*" sau, conform lui Gary Johns, "*organizațiile sunt invenții sociale pentru atingerea obiectivelor prin eforturi de grup*". Deși simplistă, definiția aceasta acoperă o largă varietate de grupuri organizatorice, cum ar fi cele din mediul de afaceri, învățământ, sănătate, asociații, culte religioase, agenții guvernamentale și aria acestora de incidență[2]. Din perspectiva teoretică de invenție socială complexă, organizația poate fi privită ca un sistem deschis, cu o dinamică și adaptabilitate proprie în funcție de scopul înființări acesteia, având un caracter probabilistic și relativ stabil, care are funcții fundamentale de autoreglaj și organizare proprie.

Mulțimea organizațiilor poate fi divizată utilizând dihotomia public/privat, deci există organizații publice şi organizații private. Deși economia face o legătură între conceptul de „*organizație*" şi conceptul de „*bun*", diferențierea dintre organizația publică și cea privată nu are o bază economică asociată naturii bunurilor gestionate sau produse, ci una de natură juridică, pentru că aceasta se face prin raportarea la subiectul proprietății. Definită simplu, pentru uz managerial, organizația publică este un organism/structură sau entitate cu sau fără personalitate juridică, care se află în proprietatea statului. Aceasta poate fi reprezentată la nivel central sau local de diferite entităţi organizaționale, care sunt constituite, din perspectivă juridică, în subiect al proprietății. Din punct de vedere juridic, organizația publică poate să ia una dintre următoarele forme:

- *persoană publică*, dar fără a se face distincție față de autoritatea publică, cu rol reglementator, adică cea care organizează furnizarea produsului;

1. Anișoara Duică, *Management*, Ediția a II-a (revizuită și adăugită), Edit. Bibliotheca, Târgoviște, 2008, p.97.
2. N.K. Jain, *Organisational Behavior*, Edit. Atlantic, New Delhi, 2005, p.4.

- *persoană publică, cu statut de drept public*, dar cu o manifestare de entitate distinctă față de autoritatea publică cu rol reglementator;
- *persoană privată*, dar cu posibilitatea de a dispune de un act de putere publică;
- *persoană publică*, dar supusă unui regim de drept privat.

Intenţia de delimitare cât mai clară a diferitelor categorii asociate acestei clasificări este contracarată în practică de numeroase inovații. Forma distinctă în ceea ce privește clasificarea este mai semnificativă în anumite state, cum este cazul Franței şi al altor țări cu sisteme juridice apropiate; identificarea acestor categorii își pierde din claritate în lumea anglo-saxonă. Anglia are delimitările cele mai vagi şi cele mai interesante inovații, inclusiv la nivel local.

Numărul tipurilor de organizații publice este însă mai mare dacă se au în vedere şi alte criterii de clasificare decât cele juridice.

Analiza organizațiilor prin prisma orientării spre progres care, în altă ordine de idei, reprezintă profitul, sugerează un mod de raportare la un tip specific de rezultate, în principal de natură economică. Organizațiile din sectorul privat prezintă orientarea cea mai clară spre rezultate, atât prin scopurile urmărite, cât şi prin modul şi mijloacele utilizate până la atingerea acestora. Dacă aceste organizații au o natură comercială, atunci orientarea spre profit devine esențială în comportamentul lor, chiar dacă operează pe o piață reglementată, care impune restricții privind maximizarea sau modul de maximizare al acestuia.

Translatarea analizei în cazul organizației publice evidențiază comportamentul diferențiat al acestei categorii, dar şi al tipologiilor de bază enunțate anterior. Organizația publică apare ca fiind orientată mai curând spre realizarea bunăstării sociale decât a profitului economic, iar organizația privată apare ca fiind orientată spre un câștig de care să beneficieze un număr restrâns de persoane, câștigul fiind, de regulă, de natură materială. În unele cazuri, se punctează faptic

organizația publică drept un colectiv de oameni care realizează bunuri *"de care beneficiază mai mult oamenii din afara organizației decât cei din interiorul ei"*[1]. Aceste organizații sunt cele care furnizează bunuri sau servicii publice sau private, care nu au ca rezultat o remunerare directă din partea beneficiarului. Acestea sunt generic cunoscute de noi ca instituțiile plătite din bugetul de stat, precum guvernele sau agențiile guvernamentale, respectiv instituțiile publice, de regulă din mediul administrativ al statului. Desigur, când vorbim despre bunuri sau servicii oferite de aceste entități, ne referim la acelea care sunt recunoscute a fi esențiale și fără de care organizația, chiar și statul, poate intra în colaps (*economic, legislativ, tehnologic șamd.*).

Revenind în sfera de analiză a organizației, cu toate că acest subiect va fi dezvoltat la finele acestui capitol, doresc să menționez că orice sistem informațional operează în contextul a două medii, unul intern și unul extern. Acestea influențează fundamental modalitatea prin care sistemele sunt conduse în scopul furnizării de servicii către beneficiarii finali sau terțiari. Pentru a recompensa eforturile aduse în organizație, atât zona de management cât și cea de execuție, trebuie să împărtășească aceeași viziune clară privitor la impactul pe care îl au în comun asupra operațiilor finale.

O posibilitate de analiză a relaţiilor dintre mediu şi organizații vizează identificarea acelor caracteristici ale mediului care ar putea explica, în mod potențial, diferențierea organizațiilor, respectiv adoptarea unor reacții şi comportamente specifice. Din această perspectivă, un prim set de indicatori de caracterizare a mediului este raportabil la următoarele dimensiuni: predictibilitatea; diversitatea; orientarea mediului față de organizație şi stabilitatea[2]. Așadar această analiză nu poate fi făcută fără să se cunoască în detaliu analiza mediilor specifice fiecărei organizații.

1. Anișoara Duică, *op.cit.*, pp.19-21.
2. Mihaela Vlăsceanu, *op.cit.*, p.91.

Din punct de vedere al managementului, atât mediul intern al organizației cât și cel extern, cer aceeași atenție din partea conducerii. Prin construcție, mediul intern cuprinde totalitatea factorilor de influență din interiorul organizației. Referirea se face cu precădere la factorii funcționali ai sistemului, precum sunt structura acestuia, cultura în care se materializează și funcționează sistemul de management, valorile organizației și ale comunității din care angajații fac parte, specificul de leadership și management al factorilor de decizie, comunicarea în interiorul și exteriorul organizației și desigur factorul tehnologic, care poate fi considerat ca parte constitutivă a mediului intern și dependință în comunicarea și relaționarea cu mediul extern.

Evidența influenței factorilor externi asupra celor interni este bine conturată în contrast cu condițiile exterioare ale mediului extern în care serviciile informaționale operează. Majoritatea organizațiilor operează în medii complexe și aflate într-o continuă schimbare, provocate continuu de apariția noilor provocări ce trebuie controlate pentru a asigura supraviețuirea și succesul. Un astfel de caz este relatat de Jimmy Wayne Spence cu privire la provocările informaționale prin noutățile informatice din perioada anilor 1978[1].

Procesul de stabilire a principalelor caracteristici pentru ambele medii - *intern și extern* -în organizație este de fapt analiza acestora în raport cu procesele organizației, rezultate care pot afecta semnificativ organizația din punct de vedere strategic.

Managementul organizației este dator să asigure un serviciu informațional performant și adaptabil la posibilele schimbări ale mediilor interne și externe. Un proces important în acest caz este compus din culegerea, asimilarea și evaluarea informațiilor inițiale din cele două medii. Printre metodele de evaluare posibile, identifi-

1. Jymmy W. Spence, „A case study analysis of organizational communication effectiveness between user-managers and information service department personnel", lucrare de disertație–Administrarea afacerilor, Texas Tech University, Texas, 1978, p.22.

căm a fi aplicabilă metoda identificării elementelor cu impact critic în rata de succes și evaluarea profilului de capabilitate (*capacitate*).

Ignorarea sau omiterea implementării unui sistem sau proces de monitorizare continuă a performanțelor organizației raportat la mediul intern și extern ar putea fi fatală sistemului de management. Declararea lipsei timpului în detrimentul finalizării unor activități mai importante și scuza minimizării costurilor este motivul pentru care aceste procedee asiguratorii nu sunt practicate, deși lipsa funcționării sistemului de monitorizare aduce un mare deserviciu sferei de planificare a altor procese (de regulă operaționale), care ar putea fi mult mai eficiente.

Deoarece prezentul studiu se concentrează pe o analiză a organizației dintr-o perspectivă a managementului informației, este necesară explicarea analizei pe segmente de interes.

Analiza organizației nu are o definiție proprie, de aceea este preferabilă o descriere schematică a celor două medii expuse mai sus în procesul analitic.

Analiza mediului exterior este influențată de diverși factori precum: factorii sociali, factorii economici, tehnologici, culturali, demografici și cei politici.

Analiza mediului interior are în procesul de autoanaliză influențe ale factorilor personalului de specialitate, serviciilor, sistemelor, resurselor și factorilor determinați de strategiile curente.

În complexul proces de analiză a organizației, regăsim și procesul de diagnoză organizațională, care constă într-o "*radiografie*" a organizației și evidențierea situațiilor existente într-o companie, identificarea activităților și proceselor funcționale și disfuncționale, pentru obținerea unei imagini corecte a modului de funcționare în acel moment al organizației. Acest proces este vital nu doar în momentele de criză, cât și în cazul proiectelor de optimizare și dezvoltare a organizației în toate subansamblele sale, aceasta vizând funcțiunea și procesele de management, comunicarea internă și externă, recruta-

rea de personal sau servicii, dezvoltarea profesională și sistemele de evaluare a performanțelor, salarizare, de gestiune a carierei. Soluțiile de analiză folosite trebuie în final să vină cu un răspuns obiectiv și comparabil pe diferite scale, precum randamentul organizației, performanța profesională, satisfacția tuturor angajaților. Chiar dacă în ultimii ani se face, în detrimentul analizei organizației prin diagnoză organizațională, o analiză a culturii organizaționale, aceasta nu oferă rezultate specifice în vederea optimizării activității organizaționale, ci furnizează doar o imagine subiectivă, recunoscută în ambele medii (*interior/exterior*) și vizibilă chiar și fără o analiză aprofundată. Această analiză a culturii organizaționale nu oferă soluții decât pentru reformarea zonei de management.

În fapt, întreaga analiză a organizației cuprinde și analiza culturii organizaționale și reprezintă harta unui întreg cadru informațional în care este asigurată securitatea și protecția valorilor organizației. Acest cadru informațional este cel mai bine reprezentat printr-o înțelegere a noțiunii de informație în organizație, a valorii și managementului acesteia.

II.2. Informația în organizație

Informația a însoțit în permanență istoria umanității, evoluția civilizațiilor şi a societăților. Importanța, rolul şi valoarea ei în dezvoltarea socială a reprezentat unul din elementele cheie ale consolidării şi dezvoltării statelor şi națiunilor. Valoarea informației ca resursă, ca mijloc de producție, ca unitate de măsură a depins însă întotdeauna de modalitățile de obținere şi evaluare, influențate într-o măsură covârșitoare de etapa de evoluție a societății la un anumit moment, precum și de mecanismele sau pârghiile folosite în obținerea, analiza şi diseminarea ei[1].

1. Adrian V. Cămărășan, *Informații clasificate – Note de curs*, Edit. CA Publishing, Cluj-Napoca, 2014, p.13.

Mediul organizațional general este clădit pe piloni fundamentali, care pot să își schimbe forma și dimensiunea, dar nu și capacitatea și rolul. Aceștia sunt materializați prin datele şi informațiile rezultate în urma activității, proceselor și comportamentului uman ale angajatului, angajatorului - persoanelor cu funcții de conducere și funcții de execuție - precum și de parteneri ori asociați. Aceste rezultate informaționale sunt percepute drept nucleul sistemului informațional general. În ziua de azi, interesul este orientat spre activitatea organizațiilor și rolul acestora în societate, acestea prezintă datele şi informațiile formale care reprezintă baza pe care se iau majoritatea deciziilor bine structurate cu rezultate pozitive pentru organizație și pentru beneficiarii serviciilor acesteia[1].

Sistemele de management organizațional contemporane nu sunt doar competitive și în continuă reinventare, acestea, din perspectivă tehnologică, migrează de la capacitatea de gestionare a volumelor limitate de informații administrate în organizație, la o automatizare bazată pe procesare de volume mari de date cu ajutorul sistemelor moderne de inteligență artificială. În acest sens, se ajunge la nevoia de cercetare a problematicii capitalizării întregului set de informații și cunoștințe existente în organizație. Motivația principală este dată de posibilitatea valorificării acestor informații și cunoștințe, în vederea dezvoltării proceselor decizionale, pentru obținerea unui grad de performanță superior. În ceea ce privește sintagma *„cunoștințe existente în organizație"* utilizată anterior, aceste cunoștințe, date și informații sunt indirect corelate cu cele existente în afara mediului intern al organizației. Am convingerea că nici o organizație nu operează strict informația generată de aceasta, mereu se fac schimburi informaționale cu mediul extern, fapt care aduce cu sine factori de performanță, dar și de insecuritate. Rezultatul acestui fenomen de tranziție și dezvoltare organizațională generală de la forma sa ac-

1. Ioan Radu, *Informatică și management – O cale spre performață*, Edit. Editura Universitară, București, 2005, p.54.

tuală spre forme tot mai mult bazate pe digitalizare, informatizare și adesea virtualizare este previzibil și de dorit. O dată cu apariția acestor rezultate, apare nevoia de reconceptualizare a triadei *date-informații-cunoștințe* în raport cu nevoia și capacitatea de gestionare a informației la nivel de conducere.

Consider că primul pas care necesită atenția noastră este stabilirea mediului în care informația este solicitată, emisă ori colectată și vehiculată, precum și a nevoilor de protecție a acesteia, ceea ce se poate executa doar prin cunoașterea aprofundată a teoriei informației în raport cu analiza organizației expuse anterior.

Pentru o mai bună înțelegere și cursivitate a acestui capitol, este necesară o segmentare a noțiunii de informație în contextul analizei organizației. Există cel puțin patru întrebări esențiale, care vor fi tratate în următoarea parte:

- Care sunt caracteristicile privind forma și conținutul informației utile?
- Care sunt factorii care determină valoarea informației?
- Care sunt modurile și canalele de comunicare a informației?
- Care sunt factorii reprezentativi în procesul de protejare a informației digitale?

II.2.1. Forma și conținutul informației utile

Forma primară a informației în organizație este reprezentată de identificarea acțiunilor sau inacțiunilor unei persoane în raport cu un eveniment, la un anumit moment în timp sau a semnalelor factorului uman[1], care odată generate pot avea un efect neprogramat sau neașteptat asupra instituțiilor publice administrative, guvernamentale sau chiar ale statului, în funcție de influența pe care această persoană o are sau a accesului acesteia la mecanisme care pot genera

1. Semnalele fizice (*expresii/microexpresii, ticuri, fizionomice*), emoționale (*stări emoționale, stări fizice datorate stărilor emoționale*) și chimice (*fiziologice, temperatură, reacții chimice*) sunt doar câteva dintre multitudinea semnalelor oferite de factorul uman.

organizației/statului un prejudiciu de imagine, sau chiar un conflict internațional. Astfel, se poate menționa faptul că atacurile și operațiunile ostile ale statelor sunt de cele mai multe ori înfăptuite prin utilizarea vulnerabilităților factorului uman, nu neapărat a sistemelor informatice. Profilarea și strângerea de informații generale privind factorul uman vizat sunt primele activități care preced desfășurarea unor campanii de amenințări avansate persistente (APT), acestea fiind cele mai utilizate metode utilizate de statele ostile pentru culegerea de informații[1]. Persoanele vizate și profilate în vederea identificării unor vulnerabilități nu sunt reprezentate doar de decidenți, acestea pot fi persoane care pot facilita indirect accesul la datele și informațiile dorite[2]. În cazul campaniilor APT se încearcă strângerea de date și informații care pot duce la identificarea, descrierea şi definirea situațiilor care cer sau par a cere o decizie. De menționat este faptul că nu întotdeauna informația căutată și sondată este cea clasificată (*secret de serviciu sau secret de stat*), ținta acestor atacuri este de multe ori organizația privată. Pentru că această lucrare atinge și subiectul activității de intelligence și pentru că foarte multe principii de funcționare ale sistemelor de securitate private sunt adaptate din practica serviciilor de informații din lumea întreagă, consider potrivită definiția emisă de W. J. Barnds, Jordan, Taylor și Korb, "*activitatea de informații presupune mai mult decât simpla descriere, ea elaborează un produs care rezultă din colectarea, relaționarea, evaluarea, analiza, integrarea şi interpretarea tuturor informațiilor adunate*". Poziția dată de această definiție activității de informații este relevantă pentru organizațiile din mediul privat, deoarece poate fi adaptată și aplicată nevoilor de securitate interne și externe, prin măsuri documentare, umane și tehnice proprii. Activitatea de informații în contextul organizațiilor

1. Adriana Dutulescu, *Interviurile* Digi24.ro, general de brigadă Anton-Mugurel Rog, directorul Centrului CYBERINT, SRI, 14.08.2020, https://www.digi24.ro/interviuri-le-digi24-ro/cine-sunt-spionii-din-telefon-si-din-calculator-interviu-cu-directorul-cyberint-anton-rog-1352811, accesat în data de 17.08.2020.
2. *Sisteme de camere de supraveghere, sisteme informatice, aplicații informatice șamd.*

privvate nu este una de colectare a datelor și informațiilor care nu privesc managementul și securitatea organizației.

Conform afirmației lui Alvin Toffler (1990) și a altora, care contextual folosesc cuvinte ce nu sunt sinonime, precum "*date*", "*informații*" și "*cunoștințe*", interschimbate prin lucrări "*pentru a evita obositoarea repetiție*"[1] pe când fiecare dintre acestea trei au o semnificație aparte în procesul informațional. Informația este un flux de mesaje, respectiv date, în timp ce cunoștințele sunt generate chiar de aceste fluxuri de informații, ancorate în credințele și convingerile deținătorului acestora[2].

Există trei dimensiuni sub aspectul cărora trebuie să privim informația obiectiv, anume dimensiunea timpului, a conținutului și a formei, care la rândul lor au alte câteva planuri de exprimare a atributelor acestora.

Deoarece, de cele mai multe ori, informația este dependentă *temporar,* avem cel puțin patru *forme de timp*:

- *Planificare*: Furnizarea informației trebuie făcută cu operativitate în momentul potrivit, atunci când este nu doar solicitată, ci și necesară;
- *Actualitate*: Calitatea deciziei stă de cele mai multe ori în calitatea dată de o informație actuală la momentul recepționării acesteia de către decident/beneficiar;
- *Frecvența*: Importanța informației este dată de utilitatea acesteia într-un anumit interval de timp, când aceasta are efect maxim în actul decizional;
- *Moment de timp*: Informația are capacitatea de a influența interpretarea unui eveniment derulat în trecut, de a conceptualiza sau crea o opinie obiectivă asupra unui fapt prezent sau despre o viitoare decizie.

1. I. Nonaka, H. Takeuchi, *The knowledge-creating company – How Japanese companies create the dynamics for innovation,* Edit. Oxford University Press, New York, 1995, p.8.
2. *Ibidem*, p.58.

De asemenea, în ceea ce privește *forma informației* sunt cinci aspecte care pot fi luate în calcul:

- *Claritatea*: Informația este lipsită de ambiguitate și livrată într-o formă simplă și inteligibilă către destinatar;
- *Granularitatea*: Informația este emisă într-o formă detaliată sau sumară;
- *Secvențialitate*: Informația este livrată modular, în secvențe predeterminate, ca la final să fie obținută în integralitatea sa;
- *Modalitatea de expunere*: Informația preia forme simple, precum orală, vizuală, auditivă, numerică, tangibilă, grafică șamd;
- *Suport*: Informația poate fi livrată în general pe suport digital și în format fizic, dar acest lucru nu înseamnă că nu există și forme bazate pe percepția senzorială vizuală, auditivă, chinestezică, olfactivă și gustativă.

În materie de *conținut* al informației, aceasta trebuie să țină cont de următoarele aspecte:

- *Acuratețea*: Informația este exactă și concisă, purificată de erori și confirmată;
- *Relevanța*: Informația este cerută contextual, drept urmare trebuie să fie utilă emiterii unei decizii obiective;
- *Completitudine*: Informația este supusă regulilor de deducție și poate fi demonstrată, având un caracter revelator și obiectiv în raport cu solicitarea beneficiarului într-un anumit context.
- *Conciziune*: Informația este livrată punctual, dar nu limitat în raport cu solicitarea beneficiarului de drept;
- *Obiectiv*: Informația are în permanență un scop general, care se poate restrânge spre particular, cu un interes intern sau extern, pe o direcție ascendentă sau descendentă;

- *Performanța*: Informația este un rezultat al performanței în raportul de finalizare a activității - a desfășurătorului activității și a resurselor utilizate sau acumulate[1].

Aspectele de formă și conținut ale informației mai sus menționate reprezintă un etalon ideal, dar în realitate informația rareori este obținută într-o formă care să corespundă tuturor acestor caracteristici.

Deoarece nu toate informațiile îndeplinesc cerințele optime în vederea utilizării acestora și pentru că nu toate induc același efect decizional, în cazul în care informației îi lipsesc anumite caracteristici, sau în cazul în care informația este ambiguă ori îndoielnică, aceasta trebuie reintrodusă în procesul de analiză a datelor și verificată, pentru ca în final să poată fi utilizată corespunzător.

II.2.2. Valoarea informației

Informația, datele, precum şi costurile şi beneficiile rezultate în urma prelucrării informației devin din ce în ce mai mult transnaționale[2]. Informația reprezintă în orice domeniu de activitate - *academic, cercetare*[3], *inovare, industrie, administrație*[4] *locală sau centrală, guvernământ, legislativ, securitate națională*[5] *șamd.* - o resursă incontestabilă, cu o valoare adesea incontestabilă și inestimabilă, completată adesea de sisteme de stocare şi procesare, care poate furniza un cert avantaj în gestionarea evenimentelor sensibile sau conflictelor închise sau deschise.

---

1. Ofelia Hobincu, „Caracteristicile informaţiei", martie 2008, http://www.perfect-service.ro/intelinet/2008/martie/intel%28i%29net.php?legatura=2, accesat în data de 19.06.2016.
2. Dumitru Iancu, „Informația Sursă de avantaj concurențial" în *Anuarul Academiei Forțelor Terestre "Nicolae Bălcescu"*, 2007, http://www.armyacademy.ro/biblioteca/anuare/2007/a21.pdf, accesat în data de 23.07.2019.
3. Georgeta Ghenghea, Zinaida Stratan, Natalia Zavtur, „Impactul culturii informaţiei asupra utilizatorilor doctoranzi (studiu de caz)", 2019, pp.42-45, http://repository.utm.md/handle/5014/1667, accesat în data de 23.07.2019.
4. Țicu Dorina, *Politicile publice. Raționalitate și decizie în spațiul administrativ*, Edit. Adenium, Iași, 2014.
5. Mireille Rădoi, *Serviciile de informații și decizia politică*, Edit. Tritonic, București, 2003, pp.33,103,164.

Utilitatea informației este dată într-o mare măsură de capacitatea acesteia de a avea un impact crescut în momentul folosirii acesteia de către posesorul de drept. Cu cât informația este mai recentă, atent verificată și validată din punct de vedere al legalității modalității de obținere ori a credibilității asumate a sursei, putem spune că valoarea informației crește proporțional, atât din punct de vedere operațional, cât și strategic. Adesea se utilizează atacuri directe sau indirecte din partea competiției, rivalilor și uneori a aliaților, care au ca obiectiv obținerea de avantaje operaționale sau strategice din sabotarea bazelor de date și exfiltrarea de date și informații sensibile[1]; „*impactul unor asemenea acțiuni poate fi devastator*"[2]. Totuși, adevărata valoare o oferă beneficiarul de drept al informației - *decidentul care a solicitat obținerea și analiza acesteia* - deoarece el este cel care poate să o cuantifice în concordanță cu baza nevoilor sale instituționale. Paradigma valorilor atribuite informației este de mult timp discutată atât la nivelul operațional cât și decizional, deoarece considerațiile sunt diferite, dându-i-se o valoare diferită în funcție de contextul în care aceasta apare. De foarte multe ori, o informație de sine stătătoare și justificată prin contextul prin care ea apare ca fiind de un grad de importanță ridicat, la nivelul decidentului, această informație, conexată la o alta, își pierde din calități, oferind de multe ori doar o altă perspectivă asupra utilității acesteia.

O altă perspectivă a valorii informației este cea dată de motivația războaielor informatice, termen care se referă la o varietate de subiecte şi este folosit în mai multe feluri, astfel că definiția sa este ambiguă. Mulți folosesc acest termen când vorbesc despre utilizarea tehnologiilor informaționale moderne în război şi astfel leagă războiul informatic de concepte precum războiul bazat pe rețea şi de revoluția tehnologică în problemele militare. Pe de altă parte, termenul se poate

1. Clifford Paul Stoll, *The Cukoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, New York, Doubleday, 1989.
2. Ioana Vasiu, Lucian Vasiu, *op.cit.*, p.160.

referi şi la lupte politice ori propagandă pentru obținerea controlului asupra fluxului şi interpretării informației, astfel încât victoria să fie asigurată prin manipularea opiniei publice naționale şi internaționale. În acest sens, atacurile informatice fac parte oarecum din războiul psihologic. Termenul este folosit contextual când se vorbește despre războiul cibernetic şi despre posibilitatea atacurilor asupra sistemelor informatice - cu preponderență cele de interes în sectorul securității naționale. În toate aceste cazuri, utilizarea termenului reflectă opinia generală potrivit căreia cheia succesului în războaiele contemporane constă la fel de mult în culegerea şi folosirea informației ca în puterea de foc[1].

II.2.3. Moduri și canalele de comunicare a informației

Bineînțeles, informația, începând cu identificarea ei, până la diseminarea și utilizarea acesteia în diferite medii de către beneficiarii de drept ai acesteia, va fi supusă prelucrării printr-un transfer controlat (fizic sau electronic) prin sistemul informațional al organizației, transfer influențat de cele mai multe ori de factorul uman. Informația vehiculată poate suferi modificări (îmbunătățiri, completări sau alterări) în timpul gestionării acesteia, motiv pentru care consider mai mult decât necesară utilizarea semnăturilor, respectiv marcarea fizică sau digitală la fiecare accesare a acesteia. În subcapitolele următoare va fi tratată și problematica sistemului informațional în detaliu.

Orice informație apare prin sistemul senzorial uman la nivelul intelectual al individului, unde am identificat un număr de șase filtre, care influențează integritatea informației. Informația suferă modificări într-o ordine logică:

- prima modificare apare în momentul identificării și a percepției acesteia ca informație sau set de date;

1. Paul Robinson, *Dicționar de securitate internațională* (traducere Monica Neamț), Edit. CA Publishing, Cluj-Napoca, 2010, pp.168-169.

- a doua oară este influențată de viziunea persoanei care o culege asupra contextului din care o extrage;
- în cea de-a treia etapă, este supusă unui set de modificări prin interpretarea acesteia într-un context util pentru cel care procesează informația;
- a patra etapă este cea în care informația necesită o cosmetizare (*de formă sau de conținut*) pentru a putea fi livrată beneficiarului și înțeleasă de acesta;
- a cincea modificare apare la nivelul percepției și interpretării beneficiarului pentru o utilizare a acesteia într-un context potrivit, acest pas este definitoriu, aici se stabilește valoarea informației în raport cu nevoile sistemului informațional;
- cea de-a șasea etapă constă în procesarea informației prin identificarea utilității acesteia într-un sistem informațional, unde își va aduce aportul prin influențarea rezultatelor din acel proces în cel mai eficient mod cu putință[1].

Informația poate lua cinci forme senzoriale (**V**izual, **A**uditiv, **C**hinestezic, **O**lfactiv și **G**ustativ) și cel puțin o formă extrasenzorială - electrică sau energetică. Cel mai adesea datele și informațiile sunt discutate în grupuri de lucru formate din două sau mai multe persoane, care au un interes legitim și dreptul de a intra în posesia acestora prin respectarea principiul *„dreptului de a cunoaște"*. În acest caz, dacă informația culeasă și prelucrată nu este clar formulată sau bine înțeleasă, aceasta poate fi supusă discuțiilor fără a lăsa semne de întrebare. În ceea ce privește sistemele de comunicare a informației, avem cel puțin trei tipuri:

- Căi de comunicație directă (*comunicări, întâlniri, ședințe, conferințe șamd.*);
- Căi de comunicare fizice (*documente pe suport de hârtie, imprimate, fotografic șamd.*);

1. De menționat este faptul că aceeași informație poate fi utilizată în mai multe contexte, procese, de către mai multe entități pentru obținerea a diverse rezultate.

- Căile de comunicare prin sistemele electronice (e-*mail, camere de discuții online, teleconferințe, videoconferințe, înregistrări, documente în format electronic șamd.*).

Deoarece tehnologia informației și a comunicațiilor a evoluat, în ziua de azi au rămas propuse spre utilizare și dezvoltare doar două dintre acestea, căile de comunicare a informației directe și cele transportate prin intermediul tehnologiilor moderne de comunicare, motivate fiind în primul rând de vastul portofoliu de tipuri de comunicații ce pot fi folosite oriunde în lume în timp real la un raport calitate / cost incomensurabil mai mic.

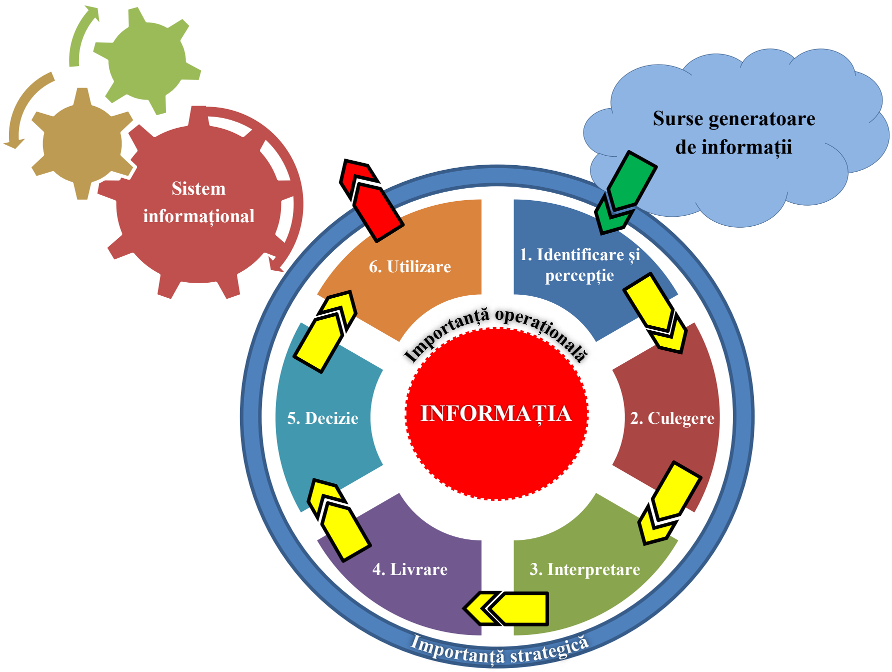


Figura nr.12. Modificările suferite de informație în ciclul de viață al acesteia

În ultimul deceniu, necesitatea utilizării canalelor de comunicații virtuale este cu atât mai mare cu cât folosirea tehnologiilor de co-

municații moderne (*telefoane inteligente, calculatoare portabile, ceasuri inteligente, ochelari inteligenți șamd.*) a crescut și este accesibilă tuturor.

Comunicarea cu ajutorul internetului sau a sistemelor GSM este atât de ușor de accesat încât nu se mai justifică pierderea timpului și a resurselor pentru a nu folosi acest sistem informațional global.

Evoluția organizației moderne este strâns legată de această transformare a mediilor de comunicații electronice, medii care formează corp comun și sunt azi elemente fundamentale ale existenței acestor organizații.

II.2.4. Protejarea informației vehiculate în mediul virtual

Informația ocupă, din punct de vedere al importanței în organizație, cel de-al doilea loc, imediat după resursa umană, fiind un bun primar al organizației. Informația este, în context organizațional contemporan, un bun sau o valoare care necesită un grad ridicat de protecție în vederea asigurării rezilienței, continuității în afaceri, pentru a reduce efectul riscului şi a mări exponențial beneficiile şi oportunitățile de afaceri. Analizând paradigma de securitate cibernetică realizăm că, deși intruziunile informatice aduc adesea mari costuri nejustificate, majoritatea organizațiilor afectate în continuare nu alocă resurse (*financiare, umane, procedurale*) suficiente pentru a se proteja. În general, organizațiile au în vedere abordarea implementării și asigurării „strictului necesar", asumându-și, într-o oarecare măsură, eventualele atacuri, breșe de securitate sau scurgeri de informații. Cu toate acestea, măsurile insuficiente luate pentru protecția datelor este motivată de organizații aproape de fiecare dată prin lipsa de resurse financiare sau printr-o viziune diferită a organizației asupra securizării informației, unde, din punct de vedere al priorităților, securitatea ocupă un loc neglijabil sau chiar neînsemnat. Paradigma de securitate este în schimbare, dinamica este dată în egală măsură de importanța din ce în ce mai mare acordată progresul tehnologiilor și sistemelor de

securitate a informației, care capătă azi valențe mult dimensionate față de acum zece ani, de care depinde aproape total succesul unei organizații, comunități, societăți și în general a oricărei țări moderne.

Pentru a putea lua în considerare prevenirea faptelor antisociale care pot avea loc în domeniul cibernetic prin instrumentarul tehnologiei informației, trebuie în primul rând să avem în vedere caracteristicile principale ale securității IT[1], caracteristici regăsite în acest capitol, la care doresc să mai adaug încă două caracteristici relevante în domeniul protecției informației, anume *amenințarea,* care de regulă ia forma unui incident de securitate nedorit cu o oarecare probabilitate și *riscul,* care este determinat de o posibilitate estimată a unei amenințări iminente.

O dată cu apariția noțiunii de „*cibernetică*", iar ulterior de „*virtualizare*", apar noi oportunități și instrumente în arsenalul infractor tradițional. Inițial acestea au depus un efort colosal pentru a putea transpune infracțiunea dintr-un plan în altul, dar cu trecerea anilor tranziția este aproape completă, infracțiunile sunt aproape perfect ajustate mediului informațional, iar infractorul și-a dezvoltat un nou simț, care îi permite oarecum intuitiv să comită fapte cu un efort mult diminuat față de „*clasici*"[2]. Țin să menționez că protecția informației nu trebuie concentrată exclusiv față de factorii externi, ci și față de cei interni, deoarece, pe lângă factorul de risc uman, există și instabilitatea echipamentelor folosite în sistemul informațional, care poate crea evenimente și incidente de securitate destul de serioase pentru a opri productivitatea pe o anumită perioadă de timp. Această protecție se face cu ajutorul unei serii de procese puse în practică de un management al securității informației, fără de care informația nu poate, ci sigur își va pierde valoarea. Acest sistem de

1. Gh. Alecu, Al. Barbăneagră, *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic,* Edit. Pinguin Book, București, 2006, pp.188-189.
2. George M. Șinca, „Cibercriminologia - O analiză succintă a fenomenului de tranziție de la criminalitatea tradițională la cibercriminalitate", în *AGORA International Journal of Juridical Sciences*, Nr. 1, Oradea, 2015, p.66.

protecție a informației este mai bine descris în capitolele următoare, care tratează acest aspect atât sub formă teoretică, cât și practică.

Din perspectiva conștientizării riscurilor și vulnerabilităților aduse de progresul tehnologic în sectorul cibernetic, trebuie menționate implicațiile aduse de parteneriatele sectorului public-privat și militar. În perioada 16-17 aprilie 2015, Olanda a găzduit Conferința Globală privind Spațiul Cibernetic - Ediția a IV-a G.C.C.S. 2015, care s-a finalizat cu adoptarea Declarației de la Haga, în cadrul Forumului Global asupra Expertizei Cibernetice (G.F.C.E.)[1]. Cu ocazia acestui eveniment, s-au punctat cele mai remarcabile rezultate din domenii diferite ale guvernării securității spațiului cibernetic şi s-a deschis o platformă de discuții cu privire la aspectele cheie ale domeniului cibernetic, unde în urma dezbaterilor s-a obținut o viziune strategică integrată a problemelor actuale, respectiv idei şi instrumente practice pentru statele participante.

România, fiind unul dintre promotorii inițiativei olandeze privind „Coordinated Vulnerability Disclosure"[2], a participat activ în organizarea evenimentului, alături de Olanda, Ungaria şi compania Hewlett Packard. Cu prilejul acestui eveniment, s-au recunoscut rezultatele auditorilor de securitate cunoscuți și ca *„pentesters"*[3], care au obținut rezultate notabile în urma activităților de securitate desfășurate în verificarea infrastructurilor digitale. Centrele de cercetare, universitățile și școlile specializate în formarea adulților sunt responsabile de infuzia în câmpul muncii din ultimii ani a unui număr impresionant de specialiști de nișă în diferitele sectoare ale securității cibernetice, unde datorită performanței și pregătirii continue au apărut tot mai mulți *„ethical hackers"* (trad. eng. *„hackeri etici"*). Aceștia sunt generic identificați ca *„White Hat Hackers"*, adică experți cibernetici de nișă, pro activi în descoperirea vulnerabilităților, pe care le notifică compa-

1. https://www.thegfce.com/, accesat în data de 22.07.2018
2. Nume anterior: *„Cyber Security Responsible Disclosure"*„
3. PWNTHECODE, „Despre pentesting", https://pwnthecode.com/courses/web-application-pentesting-101/despre-pentesting, accesat în data de 02.05.2019.

niilor și guvernelor prin rapoarte de securitate, într-o formă complexă, înainte de a le publica pe canale deschise de comunicare și hub-uri de surse deschise de informații, prin aşa numita *„divulgare responsabilă coordonată”*. Așadar, cu ocazia G.C.C.S. 2015, s-a început o abordare atipică a politicii de „responsible disclosure”, care se dovedește a fi extrem de eficientă, iar procesul de divulgare a vulnerabilității și a riscurilor de securitate poate fi astfel controlat.

Ca urmare a acestor conferințe, în 23.03.2016, a avut loc la Budapesta prima reuniune a experților privind *„divulgarea responsabilă coordonată”* a vulnerabilităților din domeniul securității cibernetice, iar a doua reuniune s-a desfășurat în 10.11.2016 la București. Unul dintre cele mai importante obiectivele ale reuniunii de la București a fost reprezentat de promovarea unei culturi deschise sau a unui hub în care toți actorii de securitate din domeniu (*sector privat, sectorul guvernamental, sectorul cercetării, sectorul academic*) să își poată oferi sprijin reciproc pentru asigurarea unui schimb eficient de informații şi stabilirea unui set unitar de practici în baza experienței și a conceptului de *„Know How”*.

Desigur, acest eveniment s-a desfășurat anual, ultimul desfășurându-se în perioada 18-20 septembrie 2018 în Singapore[1].

Aceste evenimente reprezintă un pas important al colaborării sectorului civil cu cel guvernamental și militar. Deși sunt încă numeroși pași de făcut pentru a atinge un grad suficient de încredere în ceea ce privește guvernanța spațiului cibernetic, sentimentul comun de insecuritate în acest domeniu continuă să strângă tot mai mult relația dintre toate sectoarele active într-o formă sau alta din acest vast domeniu al securității cibernetice.

1. GFCE, Report „From Awareness to Implementation”, 24.10.2018, https://www.thegfce.com/documents/publications/2018/10/18/from-awareness-to-implementation, accesat în data de 30.04.2019.

II.2.5. Managementul informației electronice în organizație

În organizațiile contemporane este necesară o reconceptualizare a modelului de management al securității, prin implicarea factorului decizional în procesele care sunt desfășurate pe parcursul întregului ciclu de viață a informației vitale în organizație[1]. Sistemul de management al securității deține o relație de interdependență cu sistemele de management al informației, ale căror rezultate colaborative sunt vizibile atât în zona de producție, cât și în profilul ascendent sau descendent al organizației din analiza planului de management.

Din punctul de vedere al managementului organizației, informația este o înștiințare, care are scopul de a declanșa reacții ce determină acțiuni.

În procesul de conducere, materia primă cu care lucrează conducătorul este informația. Orice conducător analizează situații, definește probleme, ia decizii, pune în acțiune planuri, controlează modul de îndeplinire al acestora. În toate aceste activități el culege sau primește informații, le evaluează şi le prelucrează într-un proces de gândire, ajungând la o acumulare de cunoștințe cu care își creează un plan de management de succes. Rezultatul acestui proces de gândire îl reprezintă, de asemenea, anumite informații, antrenate la rândul lor în alte fluxuri informaționale pentru optimizarea întregului sistem informațional.

Succesul unei organizații depinde tot mai mult de stilul managerial prin care conducerea își culege informațiile, calitatea datelor și informațiilor culese, capacitatea de procesare a acestora în vederea livrării celor mai eficiente și potrivite soluții și desigur de rezultatele obținute din deciziile și acțiunile întreprinse pe baza acestora. Reușita procesului de conducere se bazează pe două elemente esențiale: gândirea conducătorului şi informația disponibilă[2], care poate fi regăsită în cea mai simplă formă posibilă, anume informația brută sau

1. CISCO, „Cisco 2015 Annual Security Report", p.44, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf, accesat în data de 15.08.2016.
2. Tudor Hobeanu, Loredana Hobeanu, *Management – Fundamentele managementului organizației*, Edit. Sitech, Craiova, 2007, p.125.

prelucrată, ajungând la diferite nivele de importanță și clasificare. Într-un proces de gândire există anumite date sau informații primite sau culese, informații care pot fi argumente simple sau complexe, impresii sau opinii. Toate informațiile intră în procesul de gândire de unde rezultă soluții care pot fi decizii, idei sau atitudini.

Informația brută este echivalentă cu materialul neevaluat şi neexploatat, este prima formă a oricărei viitoare clasificări a informației. Ea se poate prezenta sub formă de fotografii, filme, scheme, texte, mesaje video sau sonore șamd. Valoarea acestui tip de informații este tactică. După evaluarea şi prelucrarea informațiilor, sau mai corect a datelor, ele pot dobândi mai multă relevanță, fiind înscrise într-un context coerent.

Informația de bază este un produs de referință cu caracter factual, de origine enciclopedică şi la care se raportează întregul ecosistem național și chiar internațional din domeniul politic şi militar, economic, bancar, geografic, demografic, al resurselor și capacităților ori vulnerabilităților unei țări, comunități și adesea ale unei organizații[1].

Parafrazându-l pe Alvin Tofller, observăm că „*între instrumentele puterii cele mai importante sunt: forța, banii ori puterea financiară şi informația. Informația este elementul esențial şi cel mai versatil instrument, având în vedere că poate duce la evitarea unor situații care necesită utilizarea forței sau a banilor, putând fi folosită în a-i convinge pe ceilalți să acționeze conform motivațiilor celui care deține informația, indiferent de interesul conștient al celorlalți*”[2].

Orientativ, în 25 septembrie 2013, s-a pus în aplicare un nou standard internațional de securitate a informației, numit ISO/IEC 27001:2013[3], care îl completează pe cel vechi, ISO/IEC 27001:2005[4],

1. Nasty Vlădoiu, *Protecţia Informaţiilor. De la concept la implementare*, Edit. Tritonic, București, 2005, p.73.
2. Adrian V. Cămărășan, *op.cit.*, p.61.
3. ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, accesat în data de 18.06.2018.
4. ISO/IEC 27001:2005, ISO/IEC 27001:2005(en) Information technology - Security techniques - Information security management systems — Requirements, https://www.

migrând efectiv la un nou concept prin punerea unui accent sporit pe măsurarea și evaluarea eficienței efectuării sistemului de management al securității informației. Deoarece a fost nevoie de o atenție sporită în spectrul informației și securității acesteia la nivel de management, în contextul organizațional al securității informaționale, acest nou standard a schimbat abordarea de evaluare a riscurilor. Acesta a fost conceput pentru a se alinia altor standarde de management, cum ar fi ISO 9001:2015[1] (*managementul calității*), ISO 22301:2012[2] (*managementul continuității afacerii*), recentul ISO 31000:2018[3] (*managementul riscului*) și ISO/IEC 20000-1:2011[4] (*managementul tehnologiei informației*), pentru o optimizare a conducerii prin acestea.

II.3. Condiția informației vitale

Pentru ca informația să servească procesului de conducere și management, să stea la baza luării de decizii, este necesar îndeplinească o serie de condiții, să aibă anumite calități.

O primă condiție este ca informația să fie exactă și veridică. Informațiile nereale, intenționat sau neintenționat alterate, pot duce la decizii eronate, cu urmări nefaste în activitatea organizației, iar în cazul securității naționale poate duce la adevărate dezastre diplomatice sau instabilități politice, financiare sau societale.

O eroare de informare poate fi adesea mult mai gravă decât o eroare sau deficiență în procesul de producție.

---

iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en, accesat în data de 18.06.2018.

1. ISO 9001:2015, Quality management systems - Requirements, https://www.iso.org/standard/62085.html, accesat în data de 18.06.2018.
2. ISO 22301:2012 - Societal security - Business continuity management systems – Requirements, https://www.iso.org/standard/50038.html, accesat în data de 18.06.2018.
3. ISO 31000:2018, Risk management – Guidelines, https://www.iso.org/standard/65694.html, accesat în data de 18.06.2018.
4. ISO/IEC 20000-1:2011, Information technology -- Service management -- Part 1: Service management system requirements, https://www.iso.org/standard/51986.html, accesat în data de 18.06.2018.

Informația trebuie să fie completă. Aceasta înseamnă că ea trebuie să conțină elemente de cunoaștere ce permit conturarea unei imagini cât mai cuprinzătoare asupra procesului, evenimentului sau situației la care se referă.

O altă condiție este ca informația să fie transmisă la timp: momentul transmiterii acesteia trebuie să fie cât mai apropiat de momentul sau perioada în care s-a produs fenomenul care interesează. Specialiștii axați pe soluționarea problemelor de management organizațional subliniază prioritatea de obținere în timp operativ a informației față de obligativitatea de a fi completă. Informația parțială furnizată la timpul potrivit este mult mai utilă pentru conducere decât informația completă din punct de vedere al formei sale, obținută însă cu întârziere.

Informația trebuie să fie relevantă, adică să furnizeze elemente necunoscute sau mai puțin cunoscute celui căruia i se adresează. Un raport care confirmă pur şi simplu ceea ce conducătorul știe deja nu furnizează o informație a cărei valoare să mărească puterea de cunoaștere și să servească la fundamentarea deciziei.

Informația, de asemenea, trebuie să fie accesibilă, modul de prezentare al informației joacă de multe ori un rol deosebit. Situațiile stau total diferit în cazul în care informația primită este clară față de situația în care aceasta este confuză ori ambiguă. Trecerea de la informație la cunoaștere se poate face ușor sau cu multă dificultate, gradul de dificultate este dat de relația surse-sistem informațional-beneficiar.

Capacitatea de a se integra reprezintă altă condiție a informației, care se traduce prin capacitatea de a porni de la un set de date sau o informație brută prin procesarea căruia să se obțină o informație cu valoare adăugată, derivată de la cea primară. De altfel, unul din principiile care stă la baza unui sistem informațional modern este "*minimum de informații primare - maximum de informații secundare*".

În cele din urmă, informația are valoare dacă este adresată celui care are nevoie de ea. Informarea diferiților conducători trebuie ast-

fel concepută încât să corespundă treptei ierarhice pe care se găsesc aceștia în concordanță cu natura activității şi cu competența lor în problemele respective. Printr-o analiză succesivă a informației primare şi derivate, începând cu treapta ierarhică situată în vârful piramidei de conducere şi terminând cu cea de la bază, poate fi depistată informația de prisos şi reținută numai aceea care este într-adevăr utilă fiecărei trepte ierarhice pentru a conduce eficient[1].

Managementul informației, din perspectiva securității în conceptul său general, se împarte în câteva categorii esențiale, despre care s-a discutat mult. Aduc în atenția dumneavoastră patru dintre acestea și anume *clasificarea informației* (condiții și forme), *mediile de securitate* (cu precădere mediul de securitate electronic), *protecția datelor* (prin proceduri, legi și instrumente) și *importanța acreditării unei rețele* la un anumit nivel de secretizare conform informației prelucrate și manipulate în acest sistem informațional.

II.3.1. Clasificarea informației

Cu toate că standardele naționale și internaționale mai sus enunțate clasifică informația generic pe tipologii, pentru a argumenta necesitatea catalogării și clasificări informației, în funcție de impactul produs de utilizarea eficientă sau ineficientă a acesteia în orice organizație, se consideră oportună reprezentarea și exemplificarea sistemului de clasificare a informației în sectorul guvernamental și ministerial din România.

Conform analizelor efectuate anual de autoritățile desemnate de securitate la nivelul Guvernului României, Ministerelor și organismelor care gestionează informații clasificate, indiferent de nivelul și clasa acestora, precum și ale analizelor interne ale structurilor de securitate - chiar și din mediul privat - se observă faptul că în România cultul prezentărilor orale este aproape inexistent, acesta fiind

1. Tudor Hobeanu, Loredana Hobeanu, *op. cit.*, pp.127-129.

regăsit strict în cadrul ședințelor în care se discută informații clasificate și oricum în finalul acestor convocări, ședințe, întâlniri de lucru șamd., se redactează un *„proces*[1]*-verbal"*[2]. Astfel, sistemul birocratic din România încurajează birocrația, majoritatea documentelor sau informațiilor, indiferent de formă, poartă însemne oficiale identificabile instituției emitente, însemne precum: antet, subsol, număr de înregistrare, siglă, nivel de clasificare, date privind multiplicarea. Aceste detalii sunt menționate pe documentele oficiale, deoarece sistemul dorește să poată trasa un eventual itinerar al informației, pentru a controla orice dată sau mediu în care informația ajunge. Un aspect interesant este faptul că, deși suntem una dintre țările fruntașe în ceea ce privește utilizarea tehnologiei informației, acest sistem de management al documentelor și informațiilor este unul învechit și greoi, dificil de administrat și ancorat într-o formă de birocrație ineficientă și parazitară. În instituțiile statului și în relația dintre instituțiile statului cu sectorul, utilizarea documentelor fizice este un dat, un truism. Orice încercare de a schimba acest sistem este văzută fie ca o modalitate de a face bani dintr-un proiect care în final să nu fie finalizat, fie ca o obligație instituțională care stă în picioare - fără o evoluție semnificativă - până la „primul mandat" al următorului decident financiar sau politic. Utilizarea acestui sistem de management al datelor, informațiilor și documentelor adesea are ca scop dorința de a lăsa o urmă în sistemul de management al informației sau al documentelor în organizație - predare/primire pe bază de condică, borderou cu semnătură, numele celui ce a primit documentul, data și în unele cazuri chiar ștampila instituției - pe întregul ciclu de viață al informației. O atenție sporită este acordată justificării activității

---

1. Academia Română, Institutul de lingvistică "Iorgu Iordan", *Dicționarul Explicativ al Limbii Române*, Ediția a II-a, Edit. Univers Enciclopedic. București, 1998, p.853 – *„succesiune de operații, de stări, de fenomene prin care se efectuează o lucrare, se produce o transformare, evoluție, dezvoltare, desfășurare, acțiune."*
2. lat. *verbum*=vorbă, cuvânt (*a materializa vorba -cuvântul*) / lat. *verbalis*=oral, verbal (*oratoric, verbalizat*).

emitenților și gestionarilor de informații clasificate, pe când grija față de finalitatea în sine a actului de a informa este undeva într-un plan secundar - deși acesta ar trebui să fie primul obiectiv în mecanismul de informare pentru luarea de decizii.[1]

NATO își rezervă meritul principal în dezvoltarea acestui sistem de management al informației clasificate. Clasificarea constă în etichetări specifice, diferențiate ale documentelor sau informațiilor, pe toate nivelurile, în funcție de valoare conținutului acestora. Aici identificăm, deja ancorate în legislație internațională, informațiile de interes public (*open*) sau cele neclasificate, dar nedestinate publicității (*unclassified*), cele confidențiale, precum datele cu caracter personal sau special[2], urcând spre informații secrete profesionale, secrete de serviciu şi clasa secretelor de stat din România - nivelul *„secret"* (0), *„strict secret"* (00) și *„strict secret de importanță deosebită"* (000) sau nivelurile și clasele de clasificare ale informației în spațiul UE – *„unclassified"* (UNCL), *„EU restricted"* (EU-R), *„EU confidential"* (EU-C), *„EU secret"* (EU-S), *„EU top secret"* (EU TOP-SECRET)[3].

La început, inițiativa a avut un caracter fatalist, făcându-se o asociere liniară în rândul informațiilor din clasa secretelor de stat, precum este cazul informațiilor de nivel *secret* (0), compromiterea acestora putând avea ca efecte pierderea de vieți omenești și informațiile de nivel strict secret (00) (*top-secret*), a căror compromitere poate consta în pierderea mai multor vieți omenești. Din experiența a peste 14 ani în sectorul de apărare, siguranță publică și securitate națională am

1. Ionel Nițu, *op.cit.*, pp.235-236.
2. *Datele cu caracter personal sunt prelucrate și protejate conform prevederilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date, cu intrare în vigoare prin aplicarea directă cu data de 25 mai 2018,* https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EN, accesat în data de 28.06.2018.
3. Comisia Europeană, ANNEX G - PADR SECURITY CLASSIFICATION GUIDE, „Security Classification Guide", Version 3.0, 14 March 2019, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/guide/pse/pa-guide-scg-padr_en.pdf, accesat în data de 06.08.2020.

observat că deși toți cei activi în acest sector au acces la informații clasificate, începând cu secret de serviciu și până la secrete de stat, nu toți au capacitatea de a analiza și discerne linia de demarcație între aceste informații. Cadrele active dețin autorizație/certificat de acces la informații clasificate, deoarece fișa postului o cere, bazat pe responsabilități, atribuții și alte activități diverse. Așadar, se poate ușor face o corespondență între activitățile, nevoia de a cunoaște și accesul la informații clasificate. Mai mult, se poate spune că lipsirea de acces la o anumită clasă de informații sau la un anumit nivel de secret poate duce chiar și la întreruperea raporturilor de muncă.

Accesul la toate categoriile de informații este strict reglementat momentan. În acest context, pentru exercitarea activităților de control, datele stau puțin diferit. O persoană poate avea acces la pura vizionare/lecturare a unei informații sau a unui document clasificat într-o anumită categorie de informații cu condiția primă de a avea accesul la aceea clasă și nivel de secretizare, sau superior, cu mențiunea că trebuie să fie respectat principiul *„nevoii de a cunoaște"*. Spre exemplu, o persoană cu acces la clasa de informații secrete de stat, nivel strict secret poate citi informații confidențiale, neclasificate (*nedestinate publicității*), secrete şi strict secrete, cu condiția respectării principiului *„nevoii de a cunoaște"*, iar o alta cu drept de acces la informații secrete de serviciu nu poate accesa informații secrete de stat, nivel strict secret, oricât de îndreptățit ar fi - chiar dacă acele documente și informații au fost generate de el însuși în perioada când a avut acces la informații clasificate din clasa secretelor de stat. Astfel, putem spune că informațiile pot fi accesate de persoanele cu nivel de acces egal cu cel al documentului sau superior (informația de interes public, confidențial, nesecret nedestinat publicității, secret de serviciu şi secret de stat (*SECRET - STRICT SECRET - STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ*) sau în exterior, în spectrul internațional, prin echivalarea claselor și nivelurilor de secretizare (*SECRET NATO* sau *TOP SECRET*). Informațiile dintr-o clasă și nivel

superior de secretizare pot fi accesate de persoane cu un acces inferior numai prin adoptarea deciziei de declasificare din partea emitentului sau a celor îndreptățiți să o facă și cu respectarea principiului general valabil al „nevoii de a cunoaște".

O dată obținută, informația poate să rămână în forma și la valoare ei inițială sau poate să sufere transformări de conținut sau de format (*din format fizic în format electronic sau invers*) ori de clasificare, precum este informația clasificată, care uneori este eronat clasificată, fiind regăsită într-o formă sub-clasificată sau supra-clasificată, fără a se ține cont de faptul că nivelul secretizării se dă contextual de valoarea informației.

Clasificarea informației pe clase și niveluri se întâlnește de regulă în mediile instituțiilor publice, militare, guvernamentale - prea puțin se regăsesc informații cu un nivel de clasificare peste cel reglementat ca secret de serviciu în organizațiile din mediul privat. Totuși, întâlnim și excepții. Cu toate acestea, organizațiile nonguvernamentale nu sunt limitate în ceea ce înseamnă adaptarea acestor norme, metodologii și tehnici în sistemul informațional propriu.

Clasificarea este acea acțiune de limitare a accesului la o informație datorită posibilelor efecte produse de diseminarea neautorizată a acesteia. Ne referim exclusiv la măsuri de securitate, care nu schimbă deloc conținutul sau forma informației. „*Obiectul*" de protejat îl poate constitui fie conținutul propriu-zis al informației, fie sursa acesteia. Clasificarea unui document trebuie precedată de o apreciere în privința necesității de clasificare. Un nivel prea ridicat de clasificare sistematică conduce la o diminuare a rolului acesteia. Deci, în procesul de clasificare a informaților este necesară moderația. Clasificarea nu este a priori legată de evaluare.

Supra-clasificarea (*înregistrarea unei informații, a unui document sau dispozitiv la un nivel de clasificare neadecvat conținutului printr-o clasificarea excesivă*) este total ineficientă și neproductivă. Acest lucru duce incontestabil la cheltuieli impuse de cerințele de securitate

pentru zonele de păstrare, de o creștere abuzivă și fără justificare a numărului de documente clasificate, precum şi la reducerea valorii restricționării accesului la informație. Subclasificarea presupune că, deși nu ar trebui să fie astfel, unele informații sunt accesibile. Prin urmare, clasificarea unui document ar trebui să facă obiectul unei analize serioase. Regulile formale de clasificare depind de legislația internă a fiecărui stat, însă, în mod obișnuit, nivelul sau clasa informației este marcată într-un loc vizibil pe materialul care o conține. Tipul de clasificare poate fi însoțit de un cod de distribuție, care poate să impună restricții suplimentare în funcție de beneficiari.

Se utilizează şi *clasificări speciale*, cum sunt cele folosite de Casa Albă pentru documentele de administrare internă, sau, în Marea Britanie, pentru documente cu caracter personal. Problema mijloacelor de prevenire a fotocopierii documentelor clasificate se ridică din ce în ce mai frecvent şi mai acut. Clasificarea și dreptul de acces la un anumit nivel de secretizare sunt două dintre cele mai importante aspecte care pot soluționa problema distribuției informațiilor. Astfel, nu este suficientă stabilirea unor reguli de distribuție, fiind necesară de asemenea precizarea persoanelor care au acces. În țările fostului bloc comunist informațiile care priveau în vreun fel apărarea sau securitatea erau considerate "secret" (*supra-secretizare*), rezultând o hipertrofiere a aparatului birocratic militar[1].

II.3.2. Cadru normativ și legislativ românesc privind prelucrarea datelor și informațiilor

În România, aceste proceduri sunt reglementate de legislația națională (*Decizii, Ordine, OUG, Hotărâri de Guvern, Legi șamd.*) și puse în aplicare cu ajutorul organismelor naționale (*prin funcții și structuri de îndrumare, verificare și control*) precum ORNISS, care prin calitatea

1.

sa unică exercită atribuții de reglementare, autorizare, evidență şi control în conformitate cu prevederile naționale în domeniu[1].

Este lesne de înțeles faptul că o bună parte a legislației românești (*Legea nr. 182 din 12 aprilie 2002, Hotărârea de Guvern nr. 585 din 13 iunie 2002 șamd.*) este învechită și modificată contextual prin revizuiri și actualizări. Orice act - *lege, hotărâre, regulament șamd* - care a ajuns să fie modificat în mare măsură sau a cărui conținut este incoerent ori lipsit de relevanță în actualul context tehnologic și de securitate trebuie abrogat și schimbat cu un altul care, pe de-o parte, să satisfacă prezentele cerințe și nevoi, dar care să dețină și un caracter previzionar, bazat pe experiența statelor aliate sau a celor cu o certă experiență în domeniu. În contextul de securitate național și internațional actual, precum și al legislației internaționale actualizate și ratificate, este evidentă necesitatea emiterii unui set normativ aliniat la dreptul internațional și tratatele/parteneriatele strategice și operaționale ale României în calitatea sa de țară membră a UE și aliat NATO, păstrându-se desigur suveranitatea națională.

În același context, pot face cu responsabilitate o afirmație provenită din experiența acumulată în domeniul securității informației. Este evidentă lipsa unui organism național, competitiv și modern, cu obiectivul principal de gestionare a bazelor de date și a informațiilor necesare obținerii și monitorizării accesului persoanelor sau instituțiilor la date și informații clasificate. De asemenea, putem observa nu doar lipsa de operativitate în administrarea unor aspecte ce țin

1.

- ☑ *„Legea nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate, ale Standardelor naţionale de protecţie a informaţiilor clasificate în România, aprobate prin HG nr. 585 din 13 iunie 2002;*
- ☑ *Hotărârea de Guvern nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România, şi ale Normelor privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin HG nr. 353 din 15 aprilie 2002;*
- ☑ *Hotărârea de Guvern nr. 353 din 15 aprilie 2002 pentru aprobarea Normelor privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România."*

în mod direct de gestionarea accesului la informație, cât și lipsa de resurse financiare și materiale ale instituțiilor în cadrul cărora se vehiculează informații clasificate pentru asigurarea unui nivel de securitate potrivit nivelului informației gestionate de acestea.

Privind spre o altă categorie de date, anume datele cu caracter personal și cele cu caracter special este important ca acestea să fie protejate și normate, atât la nivel instituțional, cât și la nivel legislativ național și internațional (european). Aceste date colectate, centralizate, analizate și utilizate într-un scop obscur pot duce la apariția unor informații a căror pierdere, divulgare sau diseminare poate aduce certe inconveniente[1], dezavantaje[2] sau prejudicii statului.

Din acest motiv, în România regăsim legislația în vigoare aliniată la normativele UE (*Directive, Decizii, Convenții, Recomandări, Opinii ale grupurilor de lucru, Regulamente, Standarde șamd.*) și adaptată la contextul cultural, social, politic și legislativ românesc, din care doresc să amintesc cadrul de înființare și funcționare al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal[3].

---

1. DLA Piper, „GDPR Data Breach Survey:February 2019", https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf?la=de&hash=C9DD3CB559E5F8E47E395FBB175F6965A15F771F, accesat în data de 30.04.2019.
2. David Volodzko, „Marriott Breach Exposes Far More Than Just Data", 04.12.2018, https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#1f91929d6297, accesat în data de 30.04.2019.
3.
   - ☑ *„Legea nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare – Republicare;*
   - ☑ *Legea nr. 129 din 15 iunie 2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;*
   - ☑ *Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi*

II.3.3. Criterii generale ale clasificării informațiilor în organizație

Printre criteriile generale ale clasificării informațiilor în organizație se numără și:

A. *Valoarea*: Raportându-ne la sectorul privat, putem afirma că valoarea este cea care dă nivelul de clasificare. În sectorul public, administrativ și cel militar informația este clasificată prin cuantificarea prejudiciilor, efectelor și impactului dat de dezvăluirea acesteia.

B. *Vechimea*: Raportul dintre vechimea sau actualitatea informației și importanța sau efectele acesteia este cel care denotă interesul pentru o clasificare conformă a acesteia. Fiecare clasă și nivel de secretizare are un regim special de păstrare.

C. *Uzura*: În momentul apariției unei informații care suprimă sau include informația deja deținută, aceasta devine lipsită de valoare, motiv pentru care aceasta va fi înlocuită cu alta.

---

privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);

☑ *Regulamentul de Organizare şi Funcţionare al ANSPDCP din 11 Noiembrie 2005, cu modificările şi completările ulterioare;*

☑ *Legea nr. 682 din 28 noiembrie 2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981;*

☑ *Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;*

☑ *Norme metodologice din 20 noiembrie 2002 pentru aplicarea Legii nr. 365/2002 privind comerțul electronic;*

☑ *Legea nr. 146 din 10 iulie 2008 pentru aderarea României la Tratatul dintre Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat de Luxemburg, Regatul Ţărilor de Jos şi Republica Austria privind aprofundarea cooperării transfrontaliere, în special în vederea combaterii terorismului, criminalităţii transfrontaliere şi migraţiei ilegale, semnat la Prum la 27 mai 2005;*

☑ *Legea nr. 238 din 10 iunie 2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice – Republicare, sau din legislația Uniunii Europene, Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)."*

D. *Asocierea:* are impact în clasificarea informației doar atunci când aceasta este valorificată în funcție de importanța pozițiilor, funcțiilor și calității indivizilor[1].

II.3.4. Sistemul decizional bazat pe sisteme informaționale.

Literatura de specialitate definește sistemele decizionale[2] ca fiind rețele intercorelate de decizii aplicate în sistemul organizațional[3], decizii care sunt structurate conform nevoilor și cerințelor funcționale ale organizației și organigramei sectorului decizional din organizație, cu scopul de a aduce un aport funcțional în procesul de management[4].

Cele două componente, cea informațională şi cea decizională, stau într-o balanță și nu într-un echilibru. Paradigma poate fi abordată corespunzător prin tratarea relației informație / decizie. Decizia este luată mereu în baza unui context și a unor informații, de regulă verificate și validate, astfel aceasta poate căpăta o valoare cu atât mai mare cu cât sunt îndeplinite toate condițiile de colectare, gestionare și livrare. Criteriile de valorificare a informației sunt suplimentate de raportul calitativ al informației, dat de completitudinea în momentul transmiterii, exactitate în contextul în care este solicitată, oportunitatea dată de perspectivele decidentului în a o folosi și fiabilitatea acesteia în raport cu condiția calitativă şi relevanța în luarea unei decizii, identificând aici doar elementele constitutive primare în procesul de livrare a unui set de informații coerent pentru luarea unei decizii cel puțin corecte.

1. Dumitru Oprea, *Protecția și securitatea informațiilor,* ediția a II-a, Edit. Polirom, Iași, 2007, p.71.
2. Florin Gheorghe Filip, *Sisteme suport pentru decizii*, Edit. TEHNICA, București, 2007.
3. Țicu Dorina, *op.cit.*, p.97-99.
4. Mihai Bîzoi,*Sisteme Suport pentru Decizii Bazate pe Comunicaţii* (teză de doctorat), Academia Română,

Institutul de Cercetări pentru Inteligenţă Artificială, București, 2010.

În contextul aplicabilității *teoriei deciziei*[1] în orice formă de organizare, rolul decisiv în luarea unei decizii este cel al relevanței, importanței și impactului adus de informație și asta datorită întregului mecanism care contribuie la luarea deciziei. Elementele constitutive sunt *factorii de mediu, restricțiile și limitările organizaționale, tipul obiectivelor și valorile organizaționale, stilul de management și conducere,* care își găsesc oglindite eficiența în rezultatele deciziei luate pe seama lor. *„Acest aspect fundamental face ca în procesele decizionale, alternativele aflate la dispoziția decidentului să fie determinate şi de elemente de natură obiectivă, dar şi de propriile lui limite cognitive şi informaționale"*[2].

Conceptual, noțiunea de *„sistem informațional"* se rezumă la o simplă definiție cu caracter destul de omogen și dinamic, anume că aceasta reprezintă *„ansamblul organizat și integrat al modelelor, procedurilor, resurselor umane și mijloacelor tehnice de culegere, înregistrare, prelucrare, transmitere și stocare a datelor și informațiilor cu privire la activitatea sistemului de conducere și a mediului în care funcționează acesta"*[3].

Din punct de vedere al securității care trebuie asigurată la nivelul informațional, pe lângă securitatea electronică și securitatea comunicațiilor, întâlnim și securitatea informațională care, într-o oarecare măsură, le cuprinde pe celelalte două enumerate anterior.

Securitatea informațională se referă la activitățile întreprinse pentru a împiedica informațiile secrete să ajungă în mâini ostile, dar şi la activitățile de protejare a sistemelor informaționale, cum ar fi calculatoarele, în fața unui atac. Există mai multe feluri de securitate informațională:

- *securitatea fizică*, care presupune construirea şi întreținerea structurilor fizice pentru a proteja documentele, computerele

1. Roxana Davidescu, Alexandru Trifu, „O perspectivă mentală de valoare în teoria deciziei în condiții de risc" în *Theoretical and Applied Economics*, nr. 7 (502), , Edit. Asociația Generală a Economiștilor din România – AGER, București, 2006, p.101, , http://store.ectap.ro/articole/129.pdf, accesată în data de 23.06.2018.
2. Ioan Radu și colab.,*op.cit.*, pp.65-66.
3. Tudor Hobeanu, Loredana Hobeanu, *op. cit.*, p.124.

şi personalul şi pentru a-i împiedica pe alții să le fure sau să le atace fizic;

- *securitatea documentelor*, care implică crearea regulamentelor de utilizare a materialelor tipărite cu conținut sensibil;
- *securitatea personalului*, care include proceduri precum verificarea oficialilor de intelligence şi a altor categorii de personal care au acces la informații confidențiale pentru a se asigura că nu au slăbiciuni sau obiceiuri care i-ar putea determina să dezvăluie altora informații cu caracter clasificat;
- *securitatea comunicațiilor*, care reduce probabilitatea interceptării comunicațiilor, prin reducerea emisiilor electronice şi prin criptarea datelor;
- *securitatea computerelor*, care protejează computerele de acțiuni de „*hacking*", de viruşi, viermi informatici sau alte forme de atac cibernetic;
- *inducerea în eroare*, care protejează adevărul prin determinarea altora să creadă neadevăruri
- *contra-intelligence*, care constă în măsuri mai active de a elimina, a deteriora sau de a îngreuna activitățile ostile de culegere de intelligence.

Utilizarea tot mai frecventă a tehnologiilor informaționale în ultimii 20 de ani le-a oferit numeroase oportunități celor care au în plan furtul de informație confidențială sau sabotajul sistemelor informaționale. Ca urmare, securitatea informațională a devenit tot mai importantă, atât pentru guverne, cât şi pentru corporațiile private[1].

Unul dintre elementele care asigură securitatea informației este informația care trece printr-un amplu ciclu de analiză, pusă la dispoziția și folosită de liderii politici și militari din întreaga lume - element cunoscut și ca produs de intelligence. Acest element fundamentează acțiunile generatoare de securitate atât în mediul organizațional

1. Paul Robinson, *op.cit*, pp.207.

intern, cât și în cel extern. Acest ciclu de intelligence este de fapt un proces compus din patru etape sau stadii de evoluție:

- *direcția* în care decidenții legitimi ai organizației sau ai statului însărcinează structurile sau agențiile de intelligence, indicându-le întrebările la care au nevoie de răspunsuri - necesități de intelligence;
- *colectarea*, stadiu în care organismele responsabilizate prin direcții de intelligence adună datele și informațiile de care au nevoie pentru a răspunde la întrebări, respectiv la necesitatea de intelligence;
- *analiza* este cea de-a treia etapă care solicită capacitățile de analiză și sinteză a structurilor sau agențiilor, pentru a compara, evalua și interpreta informația;
- *diseminarea* este ultima etapă, în care cei responsabilizați prin direcții în a colecta și analiza anumite informații și date raportează rezultate și concluzii către decidenții care au solicitat demararea acestui ciclu de intelligence.

În ambele sectoare (privat și public) necesitatea de a investi în *intelligence* este în raport cu nevoia de securitate existentă. Intelligence-ul este și un element de o importanță strategică desăvârșită, rezultatele obținute din acest sector reprezentând în unele cazuri chiar și o schimbare de obiective și viziune a statelor și a organizațiilor.

Cunoscând chiar și empiric ceea ce este intelligence-ul, putem să înțelegem și nevoia de *intelligence de securitate*, care se referă la un anumit domeniu de nișă, anume la aplicarea ciclului informației de intelligence în raport cu amenințările la adresa securității în contextul amenințărilor preponderent interne și prea puțin a celor venite din exterior.

Când vorbim despre intelligence de securitate, de regulă, ne concentrăm atenția pe fenomenul terorismului, crima organizată, subversiunea și spionajul și în nici un caz asupra intelligence-ului economic, politic sau militar. Intelligence-ul de securitate nu este

identic cu securitatea informațională, care are ca scop primar protejarea informației cu ajutorul întregului instrumentar de securizare a acesteia, dar este relevant în ceea ce privește asigurarea măsurilor de contraspionaj și contrainformații[1].

II.3.5. Surse generatoare de insecuritate informațională

În procesul de trecere la societatea informațională, ariile de interes general, precum economia, informația, transporturile, tehnologia şi relațiile sociale intră în sfera globalizării. Cu toate astea, societatea informațională nu va schimba esența unor domenii, ci doar funcțiile sau rolurile acestora. În această situație, funcțiile statului se vor dezvolta îndeosebi în spațiul relațiilor internaționale, al securității globale şi regionale, al comunicării gestionării sistemului de valori.

Informația a fost şi va rămâne principalul liant între oameni şi comunități. Din păcate, aceasta a fost, este şi va fi, de foarte multe ori, incorect gestionată, sau va putea fi folosită și în moduri nefavorabile societății, pentru a deservi interesele celor puțini.

În acest context, apreciez ca o caracteristică importantă extensia sau propagarea factorilor generatori de insecuritate informațională şi în domeniul economic, politic, militar și științific.

Decalajele și derapajele economice, cel puțin pe termen mediu, se vor evidenția la nivel global în anumite state cu un grad ridicat de vulnerabilitate, într-o certă măsură - *dată de analizele datelor și prognozele centrelor de cercetare* - explozia demografică se va resimți chiar și pe teritoriul statelor în care demografia este acum în scădere, calitatea mediului va scădea, iar acțiunile umane negative asupra acestuia se vor intensifica, iar lumea nu va scăpa de crima organizată, de traficanți şi de manifestări fundamentaliste, ci dimpotrivă acestea se vor înmulți. În această situație, sectorul economic național și domeniul global se numără printre agenții de susținere a dinamicii societății

1. Paul Robinson, *op.cit*, pp.112-114.

contemporane și viitoare, devenind așadar un pilon de rezistență al realității sociale, cu capacitate de influență determinantă asupra tuturor mediilor. Așadar, acesta constituie un domeniu important, care poate crea insecuritate informațională.

Globalizarea are, în virtutea legii dezvoltării societății omenești, atât componente de progres economic, informațional, cultural şi social, cât şi componente ce frânează dezvoltarea unor zone, de distrugere a identității opozanților, a valorilor unor națiuni. Se constituie așadar o sursă de insecuritate, de conflict social, uneori chiar violent.

În procesul de monitorizare şi gestionare a domeniilor de insecuritate informațională se înscriu şi acțiunile economice pentru prevenirea şi soluționarea fenomenelor de insecuritate.

Întregul ansamblu de măsuri - *metode, tehnici și tehnologii* - de securitate și securizare a informației reprezintă un complex instrument de monitorizare și control, în egală măsură a vulnerabilităților și a riscurilor regăsite în spațiul cibernetic raportat la societatea informațională. Acest ansamblu este în esență un pilon al securității naționale și al siguranței individului, respectiv a populației, indiferent dacă aceștia sunt activi online sau offline. Se subliniază în mod direct necesitatea menținerii triadei confidențialității, integrității și autenticității informației în raport cu asigurarea unui grad ridicat al disponibilității şi utilității datelor, informațiilor şi sistemelor informaționale. Triada CID, reprezintă un fundament al operațiunii de analiză și prognoză a riscului în orice context. Elementele constitutive ale triadei CID sunt:

√ *Confidențialitatea*

Confidențialitatea informației preia în acest context rolul de atribut defensiv al procesului, oferind posibilitatea generatorului de informații să limiteze accesul persoanelor neautorizate la resursele protejate. Controlul dreptului asupra datelor și informațiilor reprezintă o necesitate, care este obligatorie indiferent de forma fluxului informațional din care acestea fac parte și face referire la interzicerea

dreptul de citire, scriere sau ștergere neautorizată. În egală măsură, fie că vorbim despre secretul național sau despre secretul profesional, datele și informațiile, care prin diseminarea lor neautorizată pot aduce un prejudiciu organizației care le are în gestionare, trebuie protejate prin aplicarea oricăror măsuri necesare apărării imaginii, valorilor, resurselor și stabilității. Două elemente interdependente confidențialității datelor și informațiilor sunt identificarea şi autentificarea operatorilor acestora.

√ *Integritatea*

Reprezintă ansamblul de măsuri tehnice și umane de protecție a datelor și informațiilor care are ca scop interzicerea accesării și editării - în orice mod -, cu *mens rea* sau fără *mens rea*. Două dintre condițiile esențiale ale integrității informației sunt autenticitatea și posibilitatea identificării sursei, respectiv a non repudierii. În altă ordine de idei, integritatea este reflectată de posibilitatea identificării întregului ciclu de viață al informației, ceea ce cuprinde crearea, copierea/multiplicarea, editarea/modificarea și desigur arhivarea sau ștergerea, care trebuie să fie efectuate într-un mod legitim și autorizat. Și în acest caz integritatea informației este interdependentă principiului confidențialității, identificării și autentificării pentru un anumit proces.

√ *Disponibilitatea*

Este direct corelată cu posibilitatea necondiționată de acces a utilizatorului autorizat cu drepturi legitime la informație, prin sistemele informatice și de comunicații sau prin intermediul fluxurilor informaționale tradiționale.

Triada CID trebuie adoptată atât din punct de vedere al politicilor de securitate și al normelor interne, cât și din punct de vedere tehnic - al implementării - contextual de la organizație la organizație. Scopul sistemelor de securitate a informației este generic unul singur, de a securiza și proteja într-un mod cât mai eficient valorile, resursele și interesele organizațiilor care le adoptă pentru a-și asigura dispo-

nibilitatea, confidențialitatea şi integritatea datelor și informațiilor deținute.[1]

II.4. Managementul riscului în organizație

Efectele globalizării au adus organizațiile în fața unei noi provocări, acestea fiind nevoite să se dezvolte preponderent în sectorul cibernetic, consecințele acestei provocări pot fi catalogate ca semnalmente ale unui proces evolutiv. Desigur, prin adoptarea și abordarea acestui nou areal, datorită experienței organizațiilor, apar amenințări, riscuri și vulnerabilități în toate sectoarele organizaționale, majoritatea preluând o formă de risc cibernetic, respectiv forma unui risc informațional. Costurile derizorii cu care aceste vulnerabilități pot fi exploatate au dus la creșterea numărului de evenimente de securitate, breșe de securitate și daune financiare. *„Reevaluarea în vederea contracarării acestora nu se poate face decât printr-o mai bună guvernare a securității în mediul organizațional privitoare la riscuri şi întreg ansamblul măsurilor de asumare a responsabilității. Delegarea responsabilității riscului cibernetic către zona de execuție nu este o soluție fiabilă, aceasta este imperios necesar să rămână în administrarea şi supravegherea strictă şi directă a ariei de management, unde perspectiva elitistă trebuie să domine întregul sector de activitate și ciclul de viață al informației. Uneltele (metode, teorii, proceduri, practici exacte, intelligence șamd.) trebuie folosite pentru a expune punctual amenințările, vulnerabilitățile și riscurile cibernetice pe agenda priorităților managementului securității în organizație într-o formă reală, clară şi cu un scop concis, anume securitatea cu tot ansamblul elementelor sale constitutive.”*[2]

---

1. Ioana Vasiu, Lucian Vasiu, *op.cit.*, pp.162-163.
2. George-Marius Șinca, „Managementul Elitelor în Managementul Riscurilor Cibernetice” în *De la Elitele Securității la Securitatea Elitelor*, Edit. Presa Universitară Clujeană, Cluj-Napoca, 2017, p.65.

II.4.1. Elita, actorul de securitate și decidentul

Datorită domeniului de nișă, experții consacrați în acest domeniu sunt puțini în România, motiv pentru care procesul de colectare de date, în vederea argumentării unor opinii obiective cu privire la ceea ce înseamnă raportul dintre elită (*în sectorul cibernetic și informațional*), actorul de securitate (statal și non statal) și decidentul, a fost îngreunat și adesea limitat de aspecte precum secretul profesional, restricționarea accesului și/sau imposibilitatea diseminării informațiilor clasificate, precum și a incapacității de prezentare a dovezilor care stau la baza afirmațiilor acestora - afirmații care desigur nu se regăsesc în conținutul prezentei teze. Interviurile și dialogurile purtate de-a lungul perioadei de cercetare cu reprezentanți ai companiilor private, dar și ai instituțiilor din sectorul public, au generat o privire generală asupra procesului de securitate și securizare a informațiilor vehiculate în organizațiile din România. Persoanele intervievate pe această temă se împart în două categorii, care abordează modele diferite de guvernare a resurselor și a riscului în mediul cibernetic.

Un prim model este dat de managementul care pune accent exclusiv pe guvernarea informației prin politici de securitate, strategii de securizare a informațiilor bazate adesea pe aplicații informatice, sisteme și complexe de echipamente informatice și de comunicații utilizate în vederea optimizării infrastructurii tehnice, managementul accesului în zonele și la echipamentele de lucru, precum și monitorizare a spațiilor dedicate angajaților. Desigur, aceste acțiuni duc la o supra-securizare a spațiului de lucru, rezultând o diminuare a productivității angajaților și o creștere a dimensiunilor riscului informațional. Îngrădirea libertății angajatului la locul de muncă este un deserviciu adus organizației pe care acesta o deservește.

Având în vedere acești parametri, putem afirma că deși acest model de management este funcțional, cu siguranță nu este optim, sănătos și productiv. Elementele de insecuritate, chiar dacă nu pot fi

eliminate, trebuie diminuate, or menținerea unui astfel management, bazat pe efort susținut din partea angajatorului și a angajaților nu face decât să genereze un mediu vulnerabil, cu riscuri și amenințări neasumate. Pe de altă parte, contextual îndreptățiți, managerii delegă responsabilitatea și capacitatea decizională în ceea ce privește managementul securității și managementul riscului către zona instituțională de execuție - administrator de rețea, inginer de sistem, analist, programator. Acest aspect aduce o diminuare a responsabilizării sectorului de management al resurselor umane și management al securității, care trebuie consolidat prin sesiuni de consultanță cu *specialiștii experimentați, cercetători din domeniul securității, integratori de soluții* tehnice și de securitate, sau cel puțin cu consultanții din domeniul tehnologiei informației, securității, BI, CI, resurselor umane șamd. Rapoartele anuale de securitate ale furnizorilor de soluții de securitate consacrați la nivel global[1] arată, în urma cercetărilor din ultimi cinci ani, că ~91% din cazurile de breșă de securitate sunt strâns legate de managementul defectuos. Prima măsură propusă în aceste cazuri este de angajare a unui specialist în domeniu - un manager de securitate sau, într-o măsură completă, de înființare a unui departament de securitate, care să genereze politici, proceduri și ghiduri specifice și să implementeze, conform nevoilor de securitate a organizațiilor, într-un mod eficient atât strategic, cât și operațional, normativele interne adaptate necesităților organizației și să implementeze/monitorizeze sistemele (*software/hardware*) de *previziune - protecție - răspuns - recuperare*. Cu mici modificări de ordin cantitativ, aceste rapoarte sunt absolut valabile și în anii următori. Considerând perspectiva a fi reală, singurele variabile oscilante sunt cea de ordin calitativ și cea de ordin cantitativ.

Al doilea model este și cel mai dezirabil, unde guvernarea se face prin investirea în resursa umană și perfecționarea acesteia pentru

1. CISCO, „Cisco 2015 Annual Security Report", p.27, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf, accesat în data de 15.08.2016.

un progres organizațional sigur. Din cazuistica globală se cunoaște faptul că utilizatorii terminalelor sunt veriga slabă a securității instituției în care aceștia activează și în egală măsură sunt cel mai mare avantaj și cea mai de dorit resursă pe care organizațiile o pot avea. Rezultatele nivelului de perfecționare a angajaților în context legislativ, al standardelor, proceselor și politicilor de urmat reprezintă un barometru real și foarte eficient în cuantificarea eficienței măsurilor de securitate adoptate de organizație. Investirea în angajați se referă în mod special la certa pregătire de specializate în instrumentele de securitate a informației la care aceștia se raportează, privind utilizarea și securitatea dispozitivelor, dar și a securității spațiului de lucru (*platforme web, e-mail, servicii cloud, aplicații, programe șamd.*). În virtutea nevoii de a înțelege și analiza cât mai fidel această nevoie și nivel de pregătire a utilizatorului, prezenta lucrare are în componență un ultim capitol în care se analizează structural și inductiv nivelul de cunoștințe generale, de securitate și de risc a populației utilizatoare de tehnologie în România contemporană. Se înțelege, de asemenea, că orice formă de pregătire este bine primită de toți utilizatorii și consumatorii de tehnologie contemporană. Unul dintre cele mai motivante și importante aspecte pentru utilizatorii de tehnologie modernă este dat de faptul că majoritatea echipamentelor de comunicații utilizate azi sunt absolut necesare într-o organizație care se bazează pe fluxul de informație instant sau cu un timp de răspuns cât mai scurt, cu preponderență în mediul virtual. Fiecare dintre aceștia își asumă faptul că informația digitalizată este mult mai maleabilă și dinamică decât cea în format fizic, dar în aceeași timp mult mai vulnerabilă, astfel triada *confidențialitate - integritate - autenticitate* devenind o țintă ușoară. Metodele și tehnicile malițioase sau cu scopuri nelegitime sunt dezvoltate pentru a face față în cele mai complexe situații, contextual, fără un cert tipar, scopul fiind de cele mai multe ori unul obscur. Lipsa elitelor din acest sector de luptă împotriva criminalității cibernetice este cu adevărat o problemă de

securitate națională și internațională, granițele acesteia trecând de limita terestră, maritimă, aeriană sau spațială.

„În acest context identificăm elita, actorul de securitate și decidentul; considerând adevărat și necesar acest concept de elitism în sectorul de guvernare și management instituțional, putem afirma cu tărie că decidenții, (politici, financiari, formatori de opinie, consultanți șamd.) declarați și recunoscuți sau uneori anonimi, în spațiul virtual, pot lua cea mai înaltă formă decizională în ceea ce privește elitismul în toate sectoarele societății contemporane, influențând profund ariile în care aceștia activează sau sunt solicitați. Abordarea securității din perspectiva actului discursiv ridică întrebări, exemplificând cu relația dintre actori și analiști în procesul de definire și înțelegere a agendei de securitate."[1]

Într-un spectru general, aprecierea securității obiective este dincolo de mijloacele noastre de analiză. Principala idee este că actorii și publicul lor securizează anumite probleme într-o anumită formă a actului de securitate. Actorii care securizează nu rostesc neapărat cuvântul „*securitate*" și nici utilizarea de către ei a termenului securitate nu constituie neapărat un act de securizare[2].

Pentru a ne concentra atenția pe obiectivul principal al capitolului, menționăm rolul actorului de securitate în raportul dintre calitatea decidentului și forma elitistă pe care acesta o poate lua în vederea unei bune guvernări a informației în spațiul cibernetic ca fiind o concluzie preliminară.

Cultura de securitate cibernetică reprezintă în acest moment o necesitate și uneori chiar o obligație dată de nevoia de a îndeplini sarcinile fundamentale în orice instituție și devine o sarcină absolută a elitei, indiferent de sectorul de activitate. Cultura de securitate este un subdomeniu al culturii generale și în același timp un atribut ce ține direct de perfecționarea continuă a angajatului, fără a face referire

1. George-Marius Șinca, *op.cit*, p.67.
2. Barry Buzan, Ole Wæver, Jaap de Wilde, *Securitatea. Un nou cadru de analiză*, Edit. CA Publishing, Cluj-Napoca, 2011, pp.56- 57.

la nivelul social sau poziția ierarhică în organizație. Managementul riscului este interdependent de managementul informației, iar efectele acestora sunt în permanență cuantificate în gradul de cultură de securitate. În această ordine de idei, menționez trei trepte marcante pe scara dezvoltării culturii de securitate contemporane și anume, Societate 5.0[1], Diplomație 2.0[2] și sistemele de comunicații GSMA 5G[3], respectiv GSMA 6G, care sunt în cercetare.

Conform propunerii psihologul umanist american Abraham Maslow, în ceea ce privește bazele teoriei ierarhiei nevoilor umane, securitatea este pe locul al doilea, imediat după nevoile primare ale omului, conform *Figurii nr.13*. Așadar, cunoscând situația de fapt și observând piramida lui Maslow, se poate face o analiză de caz adaptată pe tema riscurilor cibernetice în raport cu securitatea cibernetică. Se poate ține cont și de faptul că punctele slabe, vulnerabilitățile și riscurile sunt omniprezente în orice domeniu al vieții noastre. Aceste riscuri au un impact nesemnificativ pentru societate și unul mai mult decât semnificativ pentru individ. Indiferent de magnitudine, fiind identificate în viața personală a individului, respectiv a utilizatorului și înțelegând importanța acestora, putem observa cum aceste incidente din zona personală produc schimbări la nivel interpersonal. Schimbările despre care se discută pot avea un impact minor în societate - în cazul a două persoane fără o influență în co-

1. Biroul de presă al MCSI, „Alexandru Petrescu a discutat cu Ambasadorul Japoniei în România despre soluții privind conceptul „Societate 5.0"", https://www.comunicatii.gov.ro/alexandru-petrescu-a-discutat-cu-ambasadorul-japoniei-in-romania-despre-solutii-privind-conceptul-societate-5-0/, accesat în data de 08.04.2019.
2. Ilan Manor, Elad Segev, Ronit Kampf, „Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter", în *The Hague Journal of Diplomacy*, Vol.10, nr.4, , Haga, 2015, p.331, https://www.researchgate.net/publication/283259027_Digital_Diplomacy_20_A_Cross-national_Comparison_of_Public_Engagement_in_Facebook_and_Twitter/citations, accesat în data de 09.04.2019.
3. GSMA, New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate, https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/, accesat în data de 22.04.2019.

munitate sau societate, dar pot avea un impact major când este vorba de două persoane cu influențe de necontestat în rândul populației unei țări sau a unei puteri supranaționale. Distanța dintre escaladarea unui conflict declanșat printr-o situație sau eveniment de insecuritate și până la un conflict armat este cu siguranță și rezultatul obținut datorită gradului de cultură de securitate pe care aceste persoane îl dețin. În cazuri din ce în ce mai dese, escaladarea de la un eveniment către un conflict iminent în urma unei situații de nesiguranță și disconfort, identificată la prima și a doua treaptă a piramidei, este un eveniment cu un înalt impact atât în sectorul politic, cât și în cel de apărare și securitate națională.

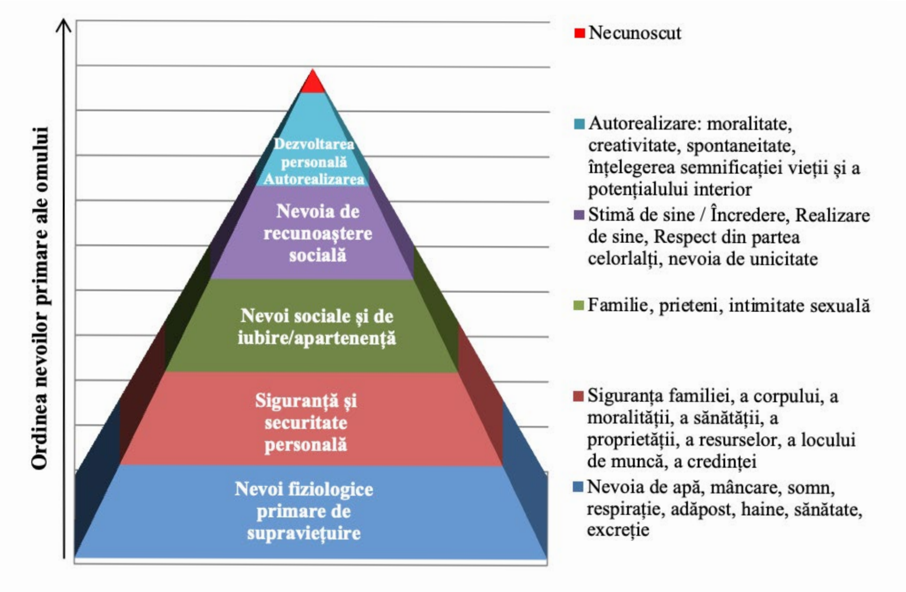


Figura nr.13. Piramida lui Maslow

II.4.2. Riscul cibernetic - Cadru de analiză

Calculul riscului este obligatoriu atât pentru a cunoaște dimensiunea resurselor necesare completării sistemului de securitate, cât și pentru asumarea unei funcționalități complete și optime a acestui sistem.

Una dintre lucrările autorului cercetării[1] analizează structurat acest cadru de analiză în contextul riscului. Consider oportună introducerea unui fragment al studiului amintit în prezenta teză.

Așadar, reflectând la problematica asumării riscurilor în sistemul informațional, observăm că, în activitatea sistemelor, procesele care se desfășoară sunt însoțite permanent de un anumit ***risc funcțional***. Astfel, prin definiția generală a riscului se înțelege probabilitatea apariției unei „*lebede negre*" - de a înfrunta o situație neprevăzută - ori de a suporta severitatea unei pagube (*pierderi*), în condițiile existenței unor pericole.

„Analizând această definiție rezultă că riscul implică atât necesitatea de a înfrunta situațiile de nesiguranță, cât și obligativitatea de a acționa rațional pentru a menține sub control incertitudinea normală a acțiunii. Pentru atenuarea și ținerea sub control a situației conflictuale este necesar să se cunoască această situație și să se acționeze pentru contracararea pericolului prin măsuri preventive sau de atenuare. În acest scop, se elaborează variante de acțiune, iar ***riscul operațional*** acceptat $R(Op_a)$ reprezintă diferența dintre eficacitatea variantei optime și eficacitatea variantei alese.

$R(Op_a)=[Ev_0-Ev_{ai}]$

unde: – i = 1,2,………,n, în care n este numărul stărilor;

– Ev_0 - varianta cu valoare optimă;

– Ev_{ai} - varianta cu valoare aleasă.

În funcție de strategia de securitate aleasă și de prețul de cost de securitate suportat, ***riscul operațional acceptat (asumat)*** poate fi calculat astfel:

$R(Op_a)\%=[1-\frac{Cs}{Cinv}]\text{x } 100$

unde: – $R(Op_a)$ - riscul operațional asumat;

– Cs - costul de Securitate suportat;

– Cinv - costul total al investiției.

1. George-Marius Șinca, „Managementul Elitelor în Managementul Riscurilor Cibernetice" în *De la Elitele Securității la Securitatea Elitelor*, Edit. Presa Universitară Clujeană, Cluj-Napoca, 2017, p.65-82.

Riscul asumat este minim în momentul în care varianta adoptată se apropie de cea optimală.

Riscurile sunt minimizate prin parcurgerea etapelor de management al riscului până la nivelul acceptabil al raportului cost/pierderi, prin implementarea de măsuri și contramăsuri conform *Figurii nr.14.*

Riscul care rezultă este riscul rezidual, care conține și uneori coincide cu riscul acceptat.

În cadrul procesului de management al riscului, în urma evaluării amenințărilor și vulnerabilităților la adresa securității informațiilor, riscul rezidual se determină după următoarea ecuație:

$$R_{\mathrm{RS}} = V\left[\sum_{x} xAx\right] - C_M$$

unde: - R_{RS} - risc rezidual de securitate;

– A - amenințări;

– V - vulnerabilități;

– CM - contramăsuri.

Firmele specializate, care au ca domeniu de activitate analiza riscului și proiectarea soluțiilor de securitate a informațiilor, cuantifică funcția V și astfel pot dezvolta sisteme de analiză a riscurilor, respectiv proiecta, realiza și implementa mecanisme de securitate a informațiilor.

Analizând ecuația de mai sus, rezultă că:

A. Nivelul amenințărilor este redus sau amplificat de cel al vulnerabilităților;

B. Valoarea acceptabilă, din punct de vedere al pierderilor, este optimală când riscul rezultat (rezidual) este egal cu riscul acceptat (asumat);

C. Valoarea riscului rezidual oglindește măsura în care nivelul și tipul contramăsurilor corespund amenințărilor și vulnerabilităților;

Figura nr.14. Managementul riscului de securitate din sistemele informaționale.[1]

D. Riscul rezidual este influențat de nivelul de cunoaștere a amenințărilor.

Practic, riscul rezidual este determinat de amenințările și vulnerabilitățile care nu au fost identificate, analiza de risc conducând la proiectarea unor sisteme de securitate care, inițial, pe baza datelor cunoscute, tratează un nivel probabil al riscului rezidual[2].

Calculul riscului, ca probabilitate de înfruntare a unei stări neprevăzute sau de a suporta pierderea, se face utilizând pentru analiză o serie de valori discrete privind posibilitățile și consecințele unor evenimente de securitate, realizându-se adevărate ierarhizări teoretice ale riscului. Întrucât riscul depinde de o serie de factori, acesta nu poate face obiectul unui model teoretic generalizat, ci trebuie determinat pentru nivelul fiecărei componente distincte (echipament, structură șamd.) a unui sistem informațional.

Practicienii consacrați duc această muncă de cercetare a determinării riscului de securitate în laboratoare performante ultradotate și proiectate special pentru a oferi un rezultat cât mai exact. La obținerea unui rezultat aceștia folosesc date obținute prin calcule verificate la rândul lor prin simulări ale evenimentelor de securitate, care stau la baza auditului de securitate, audit care trebuie făcut periodic și cu grade tot mai mari de sensibilitate.

Orice analiză de risc se va face inițial pe baza situației de securitate a obiectivului, iar în urma rezultatelor se vor determina:

A. Caracteristicile de securitate ale mediului global;
B. Structura sistemelor de securitate;
C. Integrabilitatea sistemelor de securitate;
D. Necesitățile de monitorizare strategică a securității;

1. *Ibidem*, p.235.
2. Gheorghe Ilie, Ion Ciobanu, Aurel Nour, *Confruntarea informațională și protecția informațiilor*, Edit. Detectiv, București, 2006, pp.232-234.

E. Modalitățile de operare și intervenție;

Caracteristici de revenire la normalitate după producerea unui eveniment nedorit.

Evident în etapa a doua se va face o repetare a analizei și prin compararea rezultatelor se vor evidenția eficacitatea sistemelor de securitate, vulnerabilitățile, atenuarea atacurilor maxim credibile, zonele de vulnerabilitate critică, valorile de riscuri reziduale, necesitățile de dezvoltare.

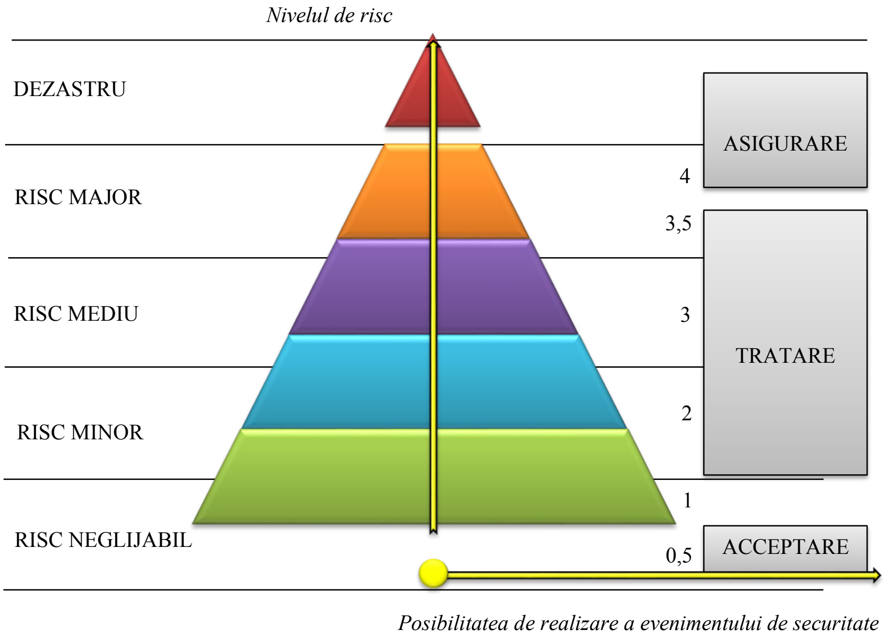


Figura nr.15. Corespondența dintre nivelurile de risc și acceptabilitatea acestora ca elemente fundamentale ale managementului riscului și al securității.

Perspectiva corespondenței dintre nivelurile de risc și acceptabilitatea acestora ca elemente fundamentale ale managementului riscului și al securității se poate observa scalar în *Figura nr.15*, care reprezintă un grafic de evidențiere a acestora.

Culegerea de informații pentru o analiză de risc este pe cât de laborioasă pe atât de necesară. Vor fi colectate și analizate hărți și fotografii, vor fi luate interviuri și măsurători, se vor face vizite la

fața locului, iar informațiile culese se vor referi la caracteristici de mediu, de amplasare, de proces, de situație socială și criminală, de comportament și de pregătire de securitate[1].

Analiza din Figura nr.15 prezintă trei atitudini posibile de risc:

ACCEPTAREA este adecvată la riscurile neglijabile, care pot produce pierderi, la rândul lor, acceptabile;

TRATAREA specifică riscurilor minore, medii și în mare parte celor majore, compensate cu adoptarea de măsuri și contramăsuri preventive care să micșoreze posibilitatea producerii evenimentelor nedorite și utilizarea de proceduri tehnice adecvate de reducere a consecințelor acestora;

ASIGURAREA este o atitudine recomandată față de riscurile dezastruoase și parte din cele majore inacceptabile, întrucât măsurile de Securitate proprii ar costa prea mult sau ar fi imposibil de adoptat datorită complexității. Acestea sunt situații catastrofale, inevitabile sau foarte greu de evitat[2].

II.4.3. Modelul cibernetic al managementului riscului

Pornind de la premisa reală că un sistem informatic și cu atât mai mult o rețea informațională digitală nu poate fi 100% securizată și în același timp utilizabilă, trec într-o zonă de competență a managementului organizațional și specific, în zona de management a riscului informației și sistemului informațional. După cum bine se știe, există mai multe metodologii privind managementul riscului, dintre acestea remarcându-se cele produse de CCTA, CRAMM, RiskPAC şi SRA. Portofoliul de management al riscului în general presupune selectarea unei suite de strategii, în funcție de aplicarea sistematică a identificării şi analizei riscurilor.

1. Gheorghe Ilie, *Riscul-Măsura Incertitudinii - Elemente conceptuale, corelații și determinări* –, Edit. UTI Press, București, 2011, p.182.
2. Gheorghe Ilie, Ion Ciobanu, Aurel Nour, *op.cit*, p. 238.

În această cursă continuă și joc al puterii, informația primează întotdeauna, riscul cibernetic depinde de veridicitatea, cantitatea și momentul livrării acesteia. Termenul „cursă" face referire la orientarea atenției la lupta pentru supremație asupra informației, în care actorii principali se regăsesc în ambele tabere ofensivă-defensivă și care îndeplinesc cumulativ o multitudine de calități, dintre care merită menționată cea de *atacator* și *apărător* al surselor generatoare de informație sau de gestionare a acesteia în sectorul informațional. *„La nivelul actual de dezvoltare a tehnologiei informației, și cu atât mai mult în viitor, utilizarea informației în forma brută sau prelucrată, s-a metamorfozat dintr-un instrument în sprijinul factorilor tradiționali de putere în cea mai dinamică dimensiune a securității naționale, fiind partea cea mai revoluționară a schimbărilor devenirii omenirii spre era informaticii și a cunoașterii"*[1].

Modelul cibernetic poate fi pragmatic adoptat la nivel managerial ca subdimensiune a modelului de management al riscului în organizație. Acest model de management al riscului, desigur, trebuie adaptat de către managerul de securitate, respectiv structurile de securitate existente, conform specificului organizației, ținându-se cont de dimensiunea, profilul și impactul asupra organizației. *„Managementului riscului îi sunt asociate multe probleme care pot constitui fie elemente de analiză, fie obiective concrete. De-a lungul timpului s-au concretizat mai multe tipuri de ierarhizări, în funcție de profunzimea cunoașterii raporturilor dintre hazard și risc, sau alte modele, dar orice model s-ar crea ținând cont de faptul că aspectele particulare sunt mult prea numeroase, nu se poate face o predicție 100% a riscului, de aceea aceasta devine cu atât mai complicată și cu atât mai greu de formalizat. Ținând însă seama că o parte din procesele de mediu, deși complicate și desfășurate în incertitudine, pot fi modelate, iar în urma excitării modelului pot fi și simulate, pentru managementul riscului poate fi asociat un model cibernetic optimal, capabil să scoată în evidență elementele de sistem (procesuale de mediu),*

1. Gheorghe Ilie, Ion Ciobanu, Aurel Nour, *op.cit*, p.18.

integrabilitatea lor funcțională, relaționarea în infrastructură, dependențele de factorii perturbatori, și să reliefeze disfuncțiunile și cauzele acestora"[1].

II.4.4. Minimizarea Riscului

Pentru a înțelege cum o organizație poate crea un ecosistem sigur din perspectiva securității informației în mediul virtual, trebuie analizat fiecare element care poate afecta abilitatea sistemelor de securitate în a preveni, detecta și mitiga riscul. O metodă sigură și aproape infailibilă este simularea și evaluarea permanentă a eficienței politicilor aplicate în organizație, acțiunilor managementului executiv, protocoalelor existente și a altor instrumente suplimentare, în vederea obținerii unei capacități reale și funcționale în prevenția, detecția și mitigarea riscului.

Elementele componente minimale ale acestui ecosistem de securitate cibernetică sunt:

- √ **Managementul executiv** este elementul primar al acestui ecosistem și stabilește prioritățile în sistemul de securitate. Acțiunile acestuia sunt definitorii în ceea ce privește mitigarea și prevenția atacurilor cibernetice.
- √ **Politicile** sunt strâns relaționate cu mitigarea. Prin aplicarea acestora asupra sistemului de securitate se controlează drepturile asupra sistemelor, aplicațiilor, funcțiilor, datelor și rețelelor de comunicații, ceea ce va afecta abilitatea sistemului de securitate de a mitiga daunele rezultate în urma breșelor de securitate. Totodată, aplicarea corectă, coerentă și contextuală a acestor politici va întări sistemul de securitate și va ajuta la prevenirea atacurilor din interior sau exterior în toate formele lor.

1. Gheorghe Ilie, *De la management la guvernare prin risc*, Edit. Detectiv/Edit. UTI Press, București, 2009, p.279.

√ **Protocoalele** corecte și necesare pot ajuta la prevenirea și detecția breșelor de securitate. Acestea sunt principalele elemente de monitorizare a fluxului informațional prin rețelele informatice, oferind și capacitatea de evaluare a nivelului de securitate existent, optim și ideal al unui sistem informatic și informațional.

√ **Instrumentele** sunt o materializare a nevoilor de securitate în ecosistemul informațional al oricărei organizații, sunt utilizate contextual și specific, conform cu primele trei elemente expuse mai sus.

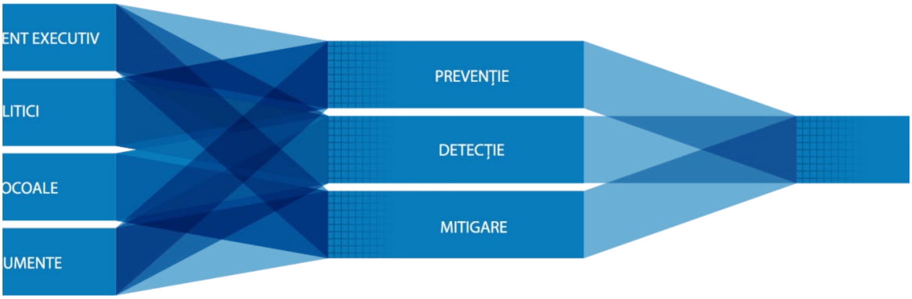


Figura nr.16. Corelarea elementelor ce asigură minimizarea riscului în organizație

Aceste trei elemente fundamentale într-un ecosistem de securitate sănătos sunt sprijinite de prevenție, detecție și mitigare, cu care sunt de fapt interconectate, între acestea existând o relație de interdependență. Personalul de securitate nu poate pur și simplu încropi la alegere un grup de lucru format din câțiva membri ai bordului executiv în vederea stabilirii unui centru operațional de protecție și securitate a organizației la atacuri, riscuri și vulnerabilități cibernetice. În acest proces trebuie implicat întregul sector de management executiv și toate elementele disponibile pentru asigurarea celei mai bune soluții. Se solicită o permanentă evaluare prin analize precum SWOT aprofundate și analize obiective privind monitorizarea în timp real a securității organizației.

În sprijinul managementului executiv, politicilor, protocoalelor și instrumentelor vin, prin relația de inter-conectivitate și interdependență, sistemele de prevenție, detecție și mitigare.

√ **Prevenția** este necesară pentru a minimiza impactul breșelor de securitate asupra organizației. Unul dintre factorii definitorii este reprezentat de angajații care, printr-o bună pregătire din perspectiva culturii de securitate, vor raporta într-un mod natural și imediat orice neregulă. Este imperios necesar ca procesele și procedurile de securitate să fie inteligibile și bine înțelese.

√ **Detecția** este un proces esențial în minimizarea impactului din breșele de securitate prin utilizarea metodelor de identificare a acestor breșe înainte ca acestea să ia proporții și să devină incidente de securitate. Pentru ca detecția să fie eficientă, este necesar ca fiecare organizație să aibă un sistem propriu de categorisire a incidentelor de securitate a informației.

√ **Mitigarea** reprezintă aplicarea unei proceduri printr-un proces de urmărire și răspuns la incidente de securitate. Deseori, acestea sunt strâns corelate cu protocoalele de management ale securității în organizație. Rezultatul acestei interdependențe este un bun management al răspunsului în momente de criză, precum incidentele de securitate cu grad ridicat de risc.

II.4.5. Predicție și previziune – Riscurile securității cibernetice în 2019

Din punct de vedere al securității de orice fel, analiza vulnerabilităților, a amenințărilor și a riscurilor (*dar acordând o mare importanță atenuării riscurilor și controalelor ulterioare în vederea prevenirii și previziunii în acest sector*) reprezintă cel puțin 40% din factorii ce conferă buna funcționare a oricărei organizații. Trebuie să luăm serios în calcul faptul că protecţia datelor informatice este o cerință legală şi operațională şi se realizează printr-un șir de măsuri, care vizează atenuarea riscurilor la adresa acestora într-o manieră completă,

aliniată cu strategia organizației, funcțională[1], echilibrată şi efectivă din punct de vedere al costurilor[2].

Totodată, dacă ar fi să simplificăm explicațiile/definițiile date riscului în cursul ultimilor ani la o ecuație simplă, aceasta ar lua următoarea formă:

RISC=[AMENINȚARE+VULNERABILITATE] **X** *VALOAREA INFORMAȚIILOR.*

Există mai multe riscuri asociate sistemelor informatice, expuse de P. Keen[3] în următoarele șase categorii:

- Conceptuale;
- Tehnologice;
- Privind implementarea;
- Economice;
- Organizaționale şi
- Legale.

De asemenea, *riscul* poate fi definit formal ca un set de perechi ordonate de consecințe potențiale *(C)* şi probabilitatea de realizare asociată *(P);* astfel

$$Risc \equiv \{(PI, CI),...,(Pi, Ci),...,(Pn, Cn)\}$$

Riscurile asociate cu sistemele informatice pot fi adresate printr-o analiză de risc şi prin implementarea unor controale adecvate (*tehnice şi procedurale*)[4]. Acest proces poate fi finalizat cu acordul și implicarea sectorului de management executiv. O bună înțelegere a obiectivelor şi funcțiilor organizației şi o abordare sistematică şi coordonată sunt

1. NIST, „Managing Information Security Risk: Organization, Mission, and Information System View", http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, 2011, p.48, accesat în data de 22.09.2016.
2. R. Anderson, B. Schneier, „Economics of Information Security, IEEE SECURITY & PRIVACY", https://www.schneier.com/academic/paperfiles/paper-economics.pdf, accesat în data de 18.04.2019.
3. Peter G.W. Keen, *Every Manager's Guide to Information Technology*, 2nd , Edit. Harvard Business School Press, 1995.
4. Vezi NIST, „Recommended Security Controls for Federal Information Systems and Organizations", http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, US Department of Commerce, 2009, p.24, accesat în data de 12.05.2017.

esențiale pentru stabilirea şi dezvoltarea unui program de management al riscurilor de securitate.

Sursele generatoare de insecuritate, prin amenințările și vulnerabilitățile evidențiate la nivelul sistemului de securitate, precum și de analiza de risc și impact a acestora, vor genera o prognoză fidelă a dimensiunii riscului asupra informației în organizație. Într-un mod sugestiv și granular, conceptele securității sistemelor informatice şi relațiilor de interdependență identificate în acest context sunt expuse în *Common Criteria for Information Technology Security Evaluation*[1].

Odată înțeleasă funcționarea managementului securității și managementului riscului, putem conștientiza necesitatea aplicării diferitelor metodologii și proceduri de securitate, de previzionare a eventualelor riscuri și de combatere a acestora. Acum mai mult ca niciodată, începând de la afacerile mici și mijlocii până la organizații și zone guvernamentale, este mai mult decât necesară impunerea unor strategii bazate pe aceste noi zone de analiză, sinteză, livrare și aplicare a normelor privind *securitatea cibernetică* și *riscul cibernetic*. Raportându-ne la ultimii trei ani, în ambele sectoare de activitate, public și privat, accesul la informație este mult mai sensibil în 2018 față de cum era acesta în 2015, fiind frecvent atacat și accesat ilegal prin metode complexe și minuțios elaborate, în special pe zone de nișă a criminalității cibernetice (*ransomware, IoT, spionaj cibernetic, machine learning, artificial intelligence și preconizez un nou tip de atac și infracțiune care va avea la bază sisteme de inteligență artificială și machine learning, cu scopul de a pune în mișcare noi tipuri de mașinării financiare, precum minarea monedelor virtuale și atacurile mult mai elaborate asupra resurselor financiare din sectorul public*). În 2017, am văzut capacitatea, gravitatea și frecvența atacurilor cibernetice la un nivel pe care

1. I. Vasiu, L.Vasiu, *Criminalitatea în cyberspațiu*, Edit. Univers Juridic, București, 2011, p.355.

nimeni nu l-ar fi putut prezice. WannaCry[1], NotPetya[2] și Locky[3] au fost unele dintre cele mai întâlnite titluri în presa scrisă sau vizuală; această importanță le-a fost acordată, deoarece hackerii au reușit să vizeze corporațiile și organizațiile pe plan internațional și lucru care le-a costat miliarde de dolari. Se consideră că în fiecare an atacurile vor avea un trend diferit, cu simptomatică și daune diferite față de cele de dinainte, dar știm că un viitor sigur este singurul mod de a preveni un mai mare impact asupra resurselor și de a asigura o prevenție mai bună împotriva criminalității informatice. În anul 2018, se presupune că există cinci arii cheie de securitate, care vor fi o vulnerabilitate pentru noi toți și pentru care trebuie să fim pregătiți[4].

A. *Rețeaua criminalilor cibernetici* este într-o evoluție ascendentă, motivată de dezvoltarea metodelor și tehnicilor utilizate, care au trecut de la cele intruzive în ceea ce privește sistemele informatice, la cele bazate pe inteligență artificială, sisteme automate și machine learning, în continuă expansiune la nivel nu doar geografic, cât și demografic. Cauzele sunt multiple, iar sursele de știri amplifică fenomenul, partea ocultă și financiară a fenomenului este ceea ce atrage cel mai tare. De exemplu, în cursul anului 2017, profitul estimat din infracțiuni cere au avut la bază soluții de tip ransomware este de un miliard de dolari americani.

B. *Minarea valutei cibernetice*, prin metode evazive, intruzive și distructive pentru echipamentele vizate, va fi în topul popularității din sectorul criminalității cibernetice în 2018. Ba-

1. Alert (TA17-132A), „Indicators Associated With WannaCry Ransomware", https://www.us-cert.gov/ncas/alerts/TA17-132A, accesat în data de 13.05.2017.
2. Alert (TA17-181A), „Petya Ransomware", https://www.us-cert.gov/ncas/alerts/TA17-181A, accesat în data de 02.07.2017.
3. Win32/Locky, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Locky, accesat în data de 10.01.2018.
4. Marcin Kleczynski, „A Look At The Five Biggest Future Cyberthreats Of 2018", https://www.forbes.com/sites/forbestechcouncil/2018/01/02/a-look-at-the-five-biggest-future-cyberthreats-of-2018/#1861a9b149d2, accesat în data de 05.01.2018.

zându-se pe progresul tehnologic de nișă, aceștia vor putea mina, nesolicitat ori autorizat, începând cu uzualele servere, sisteme informatice fixe sau mobile la întregul IoT & Cloud.

C. *Există un trend* de digitalizare în aceste zile, agresivă chiar, care vine din partea marilor organizații din toate sectoarele societății; începând cu promovarea agresivă a instituțiilor bancare de a facilita accesul la resurse, continuând cu digitalizarea și virtualizarea a tot ce se poate în sector de învățământ, până la crearea unui sistem modular în care să fie conectat orice echipament din sectorul sanitar și de sănătate publică. Există o dilemă care solicită o atenție aparte, anume, cu cât oferi mai mult spațiu confortului și fluidității, pierzi din aria de securitate și siguranță.

D. *Progresul tehnologic* în crearea de noi viermi informatici și alte sisteme malițioase, care vor fi mai greu detectabili.

E. *Atacurile asupra sistemelor* de protecție și securitate a informației atât hardware cât și software în vederea disimulării intențiilor malițioase în elemente cu nivel de încredere crescut, precum unele aplicații antivirus.

Raportul McAfee Labs din 2015 - Threats Predictions[1] a prezis noi variante *ransomware* care reușesc să evite sistemele de securitate tradiționale instalate pe sisteme, care vor viza în mod special terminalele ce au acces direct la depozitarea în soluții de tip *Cloud*, cum ar fi Dropbox, Google Drive și OneDrive, ceea ce s-a și întâmplat. Odată ce aceste obiective au fost infectate, aplicația ransomware a încercat să exploateze metodele de acces ale utilizatorilor autentificați și datele acestora salvate în partiția de date virtuală, pentru ca ulterior să ceară favoruri materiale / recompense pentru a disponibiliza informațiile către deținătorul de drept al acestora. Atacurile ransomware s-au intensificat, dublându-și numărul de la un prejudiciu de 4,1

1. Raportul McAfee Labs din 2015 – Threats Predictions, p.9, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf, accesat în data de 21.05.2017.

milioane euro în 2013 la unul de 8,8 milioane de euro în 2014. Mai îngrijorătoare este creșterea *cripto-ransomware*, care a explodat cu o creștere de 113%, de la 8,274 mil. € în 2013 la 373,342 mil. € în 2014[1], ajungând la ~1 mld € în 2017.

„Printr-un proces dinamic, alert vom ajunge la un apogeu a capacității noastre de dezvoltare a tehnologiei de prelucrare și gestionare a informației. Puterea de procesare a sistemelor informatice din ziua de azi este mult mai puternică decât a noastră, cel puțin când este vorba de strict calculul, transportul și manipularea informației. Din punct de vedere operațional, adesea găsim o sumedenie de terminale online, care nu doar că ne ușurează viața, dar care ne permit o lărgire a orizonturilor. La nivel mondial am ajuns dependenți de tehnologie, fără de care se pare că nu am mai putea evolua - sisteme critice, sisteme industriale, organizații guvernamentale și organizații private, toate stau sub umbra informației în format digital, într-un areal care este mediului fizic intangibil, unul virtual, care interconectează totul cu o interdependență impecabilă și pentru majoritate, greu de înțeles."[2]

Observând piața muncii, curriculumul școlar, activitățile extra curriculare și extrașcolare, instrumentele sistemului de învățământ contemporan în general, recunoaștem implicațiile aduse de progresul tehnologic, evidențiind tendința de utilizare în aproape orice domeniu a resurselor digitale existente și conectate la arealul cibernetic, fie că este vorba de rețeaua globală internet sau rețele independente de tip intranet. Într-o formă sau alta, majoritatea persoanelor devin parte componentă a *sistemului online*, devin componentă fundamentală a societății digitale. Analizând literatura de specialitate[3] și rapoartele instituțiilor naționale sau supranaționale europene, identificăm

1. 2015 Internet Security Threat Report, p.93, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, accesat în data de 21.05.2017.
2. George-Marius Șinca, *op.cit*, pp.65-82.
3. Colin Crouch, „Redefining Labour Relations and Capital in the Digital Age", în *Work in the digital age: Challenges of the fourth industrial revolution* (ed. Max Neufeind, Jocqueline O`Reilly, Florian Ranft), Edit. Rowman&Littlefield International, Londra, 2018, pp.187-197.

relația și gradul de dependență a vieții private și profesionale a cetățenilor europeni față de capacitatea de utilizare și gestionare a sistemelor informatice și de comunicații. Am transformat valorile tradiționale ale societății, cum ar fi socializarea și comunicarea, în valori *hibride (reale și virtuale)*, încercând să le întreținem pe ambele, fără a ține cont de costuri. Chiar și timpul limitat de care dispunem este într-o simbioză cu acest areal virtual, economisind timp pentru lucrurile cu adevărat importante nouă prin utilizarea echipamentelor electronice moderne. De asemenea, se vehiculează importanța economisirii timpului și a resurselor prin centralizarea și manipularea mecanismelor de acces a tuturor echipamentelor (*casnice, industriale, personale*) printr-o singură aplicație, sub denumirea generică de *casa inteligentă*. Progresul tehnologic a generat un nou concept în ceea ce privește sistemele automate și sistemele de comunicații, acest nou sistem se numește IoT (*The Internet of Things*)[1], care vine cu un întreg lot de riscuri, amenințări și vulnerabilități, dar și cu oportunități și beneficii. Acest nou concept duce sistemele inteligente de management al informației la un nou nivel. IoT a primit o atenție deosebită din partea firmelor ca Cisco Systems și General Electric (GE) pentru a promova dimensiunea pieței și numărul de dispozitive conectate, iar IBM vorbește despre construirea unei planete mai inteligente.

Forrester consideră că IoT este pe cale să introducă un al doilea stadiu în dezvoltarea sa, care se va concentra pe platforme de aplicații software ce oferă un nou tip de inter-conectivitate, securitate, management și capabilități de analiză[2]. Implicațiile de risc și securitate pe care aceste sisteme complexe de comunicații, de stocare de date sau de acces le aduc nu sunt de nerezolvat, dar cer o implicare activă și

1. The Internet of Things (IoT), http://www.cnbc.com/id/101411902, accesat în data de 21.05.2017.
2. Frank E. Gillett, John C. McCarthy, Michele Pelino, „Predictions 2015: Software Platforms Drive Internet-Of-Things Adoption”, ,https://www.forrester.com/Predictions+2015+Software+Platforms+Drive+InternetOfThings+Adoption/fulltext/-/E-res119422, accesat în data de 27.07.2016.

mai concentrată asupra studiilor perpetue de fezabilitate, de risc, de securitate, de analiză continuă a întregului sistem informațional în care activăm, fie în viața privată, fie în cea profesională.

În ceea ce privește utilizarea în cadrul organizațiilor a echipamentelor integrante IoT, s-a constatat faptul că odată cu beneficiile tehnologiei moderne se generează un grad ridicat de risc, greu de acceptat și mult mai greu de prognozat sau evaluat decât utilizarea sistemelor informaționale tradiționale izolate sau în rețele de comunicații de tip LAN sau WAN clasice. Majoritatea acestor echipamente sunt dotate cu module de comunicații fără fir - *wireless, GSM, Bluetooth șamd* -, acest lucru făcându-le mult mai greu de reperat și identificat în rețelele deschise utilizatorilor organizației. Odată identificată o astfel de vulnerabilitate de către un atacator, cu siguranță va fi și exploatată, iar impactul devine considerabil și poate escalada până la grava perturbare a operațiunilor de securitate, facilităților, securității fizice, securității rețelelor, protecției datelor, siguranței angajaților, clienților sau a pacienților[1]. Spre exemplu, în ceea ce privește accesarea și utilizarea sistemelor IoT prin intermediul echipamentelor mobile inteligente de comunicații - *Android, iOS, Microsoft, BlackBerry* - identificăm că cele mai mari amenințări asupra arhitecturilor IoT, în perioada 2002-2017, au fost generate de cele aproximativ 20 de aplicații malițioase, pe când doar în anul de grație 2018 aceste amenințări intenționate depășesc 20, de unde rezultă faptul că avem o creștere exponențială și explozivă a acestor tipuri de atacuri, desigur, motivată și de încrederea acordată echipamentelor IoT din ultimii ani.

Dintre cele mai vulnerabile echipamente vehiculate pe piață la ora actuală enumerăm:

1. Luana Pascu, White Paper, „The IoT Threat Landscape and Top Smart Home Vulnerabilities in 2018”, https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf, accesat în data de 23.04.2019.

- *Termostatul fără fir*[1], care odată instalat și neconfigurat corespunzător poate fi accesat de atacatori, care pot schimba temperatura pentru a supraîncălzi centrele de date, spitalele, camerele tehnice șamd.;
- *Mediile de stocare amovibile USB fără fir*[2]: în momentul utilizării fără a fi configurate conform unor politici de securitate minimale, pot duce la diseminarea neautorizată a datelor păstrate pe acesta;
- *Asistenții vocali*[3]: posibilitatea oferită de aceste echipamente de a intercepta utilizatorii acestora, fără un efort prea mare, este o vulnerabilitate peste care nu se poate trece cu vederea;
- *Camerele de supraveghere inteligente*[4] *și Televizoarele inteligente*[5]: punem în același context ambele tipuri de echipamente, deoarece, într-o mare măsură, sunt țintele aceluiași tip de atac - supraveghere neautorizată, interceptarea comunicațiilor și furt de date - televizoarele inteligente având un risc în plus, care este dat de credențialele de acces, datele bancare și alte date personale ce sunt păstrate în memoria echipamentului.
- *Dronele*[6] reprezintă o amenințare cu un grad ridicat de risc, deoarece pot fi utilizate pentru a destructura/bruia o rețea

1. Lorenzo Franceschi-Bicchierai, „Hackers Make the First-Ever Ransomware for Smart Thermostats", https://motherboard.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat, 2016, accesat în data de 23.04.2019.
2. Simon Sharwood, „A USB stick as a file server? We've done it!", 2016 https://www.theregister.co.uk/2016/08/26/a_usb_stick_as_a_file_server_weve_done_it/, accesat în data de 23.04.2019.
3. Hannah White, „Voice Assistants Are Taking Over Consumer IoT", 2019, https://www.iotforall.com/voice-assistants-consumer-iot/, accesat în data de 23.04.2019.
4. Ofer Amitai, „Why is It So Easy to Hack an IP Security Camera and Any IoT Device?", 2018, https://www.portnox.com/blog/iot/why-is-it-so-easy-to-hack-an-ip-security-camera-and-any-iot-device/, accesat în data de 23.04.2019.
5. Jason Sattler, „Threats & Research IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks", https://blog.f-secure.com/iot-threats/, 2019, accesat în data de 23.04.2019.
6. Natasha Lomas, „Venezuela claims drones loaded with explosives used in failed attack on president", https://techcrunch.com/2018/08/05/venezuela-claims-drones-loa-

informatică sau pentru a introduce în diferite zone sensibile compuși patogeni sau explozibili care pot amenința siguranța umană;

- *Imprimante inteligente*[1] sunt printre cele mai râvnite porți de acces în rețea și asta pentru că nu sunt atât de atent gestionate. De cele mai multe ori, sunt configurate o singură dată, după care nu se mai fac actualizări de drivere sau firmware, motiv pentru care sunt în topul alegerilor atacatorilor cibernetici. Aceste echipamente pot transmite istoricul documentelor imprimate și copii ale ultimelor exemplare fotocopiate sau listate, pot deschide căi de comunicare cu rețele externe neautorizat, pot fi utilizate ca mijloc de propagare a virușilor informatici sau a aplicațiilor informatice nedorite șamd.;
- *Echipamentele medicale inteligente*[2] sunt unul dintre ultimele dispozitive ce stau în atenția atacatorilor din mediul cibernetic. Obținerea de date, statistici, analize medicale și informații privind sistemul medical sunt doar câteva dintre motivele acestor atacuri. Desigur, într-o altă ordine de idei, putem spune că un atac asupra acestor sisteme și echipamente inteligente poate duce ușor la agravarea stării de sănătate sau chiar la decesul pacienților;
- *Celulele de comunicații clandestine*[3] sunt echipamente înzestrate cu un set de aplicații dedicat exclusiv impresionării celule-

ded-with-explosives-used-in-failed-attack-on-president/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=LfUMR7bPwJbLbb-M-m5hMzQ, accesat în data de 23.04.2019.

1. Kim Zetter, WIRED, „That insane, $81m Bangladesh bank heist? Here's what we know", https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/, accesat în data de 23.04.2019.
2. Zingbox, „Discovery of Cyberattack Trends Targeting Connected Medical Device - Detailed analysis of hackers leveraging device error messages", http://go.zingbox.com/rs/562-ZPO-907/images/Zingbox_Medical_Device_Cyberattack_Trend_Report.pdf, accesat în data de 23.04.2019.
3. Ionut Ilascu, „Rogue GSM Towers and Internet of Things Devices", 2018, https://www.bitdefender.com/box/blog/iot-news/rogue-gsm-towers-internet-things-devices/, acce-

lor de comunicații (de regulă GSM). Trebuie reținut faptul că celulele de comunicații reprezintă o parte componentă importantă a principiului funcționării IoT. Vulnerabilitatea rețelelor de comunicații prin sistemele 2G, 3G, 4G, 5G, LTE oferă atacatorilor posibilitatea de urmărire, monitorizare și acces la datele echipamentelor conectate la aceste celule de comunicații clandestine.

II.4.6. Capacități necesare unui management al riscului competitiv în organizațiile digitalizate

Prin intermediul rapoartelor anuale realizate pentru anul 2017 de către producătorii de tehnologie în sectorul securității cibernetice, ne sunt aduse în atenție noi tendințe și perspective de risc.[1]

Dacă în anul 2018 provocarea în ceea ce privește securitatea informației în sectorul virtual vine cu un raport de 58% din echipamentele mobile, 57 % din datele din serviciile publice de tip „*cloud*" și 57% din infrastructura „*cloud*", undeva la 57% reprezintă provocările aduse de comportamentul și cultura de securitate a utilizatorului final în sectorul virtual. Prognozând un trafic de 2.3 ZB[2] pe an până în 2020, putem spune că în următorii trei ani, începând cu 2021, acest trafic pe zi se va tripla. Trebuie menționat faptul că prin dezvoltarea tehnologică și mobilitate, ~66% din întreg traficul de internet (*făcând un calcul al IP-urilor vizibile în rețeaua internet global*) va fi realizat prin și de la echipamente mobile, precum rețele fără fir radio sau GSM, iar traficul făcut cu ajutorul echipamentelor fixe va scădea la doar ~34%.

În acest context, numerele reflectate de evoluția sectorului de comunicații GSM la nivel mondial arată că, la nivel mondial, sunt aproximativ 8.811.000.000 conexiuni mobile, cifră ce reprezintă creș-

---

sat în data de 23.04.2019.

1. Rapoartele GSMA Intelligence, Bitdefender, CISCO și Kaspersky menționate în bibliografie.
2. *Un ZB (zettabyte) este echivalentul a 1000 (EB) exabytes sau a 1 miliard (TB) terabytes.*

terea cu 6.20% a conexiunilor GSM existente din anul 2018 până în luna aprilie a anului 2019. Totodată, numărul abonamentelor GSM este de 5.106.820.000 și acesta înregistrând o creștere cu un procent de 3,72% din anul 2018 până în aceași dată a anului 2019.

La nivel național, în urma analizelor datelor culese de la cele patru mari organizații de telecomunicații voce-date din România, anume Digi Mobil (RCS & RDS), Orange, Telekom Romania (OTE) și Vodafone - excluzând celelalte rețele precum LycaMobile[1]- pentru cel de-al patrulea trimestru din 2018 se înregistrează o scădere a numărului de abonați unici cu 0.83% față de trimestrul 3, existând un număr de 26.9 milioane conexiuni, din care un procent de 46% sunt abonamente preplătite, adică cu un procent de -5.43% mai scăzut față de trimestrul 3 al anului 2018 și totuși se evidențiază o creștere a utilizării tehnologiei 3G și 4G cu 6,72% mai crescută în cel de-al 4 trimestru al anului 2018, raportându-se la un procent general de utilizare a acestor tipuri de tehnologii de 73%.[2] Până în 2025 conexiunile globale prin tehnologia 4G vor continua să înregistreze o creștere puternică, reprezentând ~60% din totalul conexiunilor GSM globale, cu o creștere de 43% față de anul 2018.

Cât despre tehnologia 5G, conform ultimelor rapoarte emise de analiștii din sectorul comunicațiilor, numărul de conexiuni cu ajutorul tehnologiei 5G va atinge 1,4 miliarde până în 2025, ceea ce va reprezenta ~15% din totalul global prognozat. Acest procent este raportat la un număr de 9.2 miliarde cartele SIM până în 2025 - incluzând aici și emisiile celor din sistemul integrat IoT. Așadar, se estimează că 5G va reprezenta aproximativ 30% din conexiunile din piețele RP Chineze și Europene, dar și aproximativ jumătate din totalul celor utilizate în SUA.

1. LycaMobile, https://www.lycamobile.ro/ro/, accesat în data de 11.04.2019.
2. GSMA Intelligence, Market Overview Report 2019, https://www.gsmaintelligence.com/markets/2859/dashboard/, accesat în data de 11.04.2019.

Numărul de conexiuni în sistemele integrate IoT la nivel mondial se va tripla, ajungând la ~25 mld. până în anul 2025, în timp ce veniturile globale din tehnologiile IoT vor crește de până la patru ori, ajungând la ~1,1 trilioane $ USD.

Un miliard de noi abonați mobili unici - luând în considerare faptul că o singură persoană poate deține mai multe abonamente - au fost adăugați în patru ani, începând din 2013, ajungând la 5,1 miliarde până la sfârșitul anului 2018, reprezentând aproximativ două treimi din populația globală.

Peste 700 de milioane de noi abonați urmează să fie adăugați în următorii șapte ani, aproximativ un sfert dintre aceștia provin doar din India.

Un număr de încă 1,4 miliarde de persoane vor începe să utilizeze serviciile internetului mobil în următorii șapte ani, astfel încât numărul total de abonați GSM prin internetul mobil va ajunge la ~5 miliarde până în 2025, adică mai mult de 60% din populația prognozată pentru acel an[1].

În acest context, observăm și faptul că viteza de transfer se va dubla, aceasta ducând la noi „*revoluții*” tehnologice, iar ~82% din întreg traficul global de internet va fi reprezentat de un trafic de date (*preponderent video*), procent care în 2015 era de ~70%[2].

În acest moment, în baza instrumentelor active și pasive de monitorizare și raportare a comportamentului echipamentelor și ale utilizatorilor în mediul online, la o medie de un miliard de activități într-o lună, identificăm un procent de 0.02% activități suspicioase, care intră de cele mai multe ori sub incidența activităților malițioase. Acest procent se compune din 58% comportamente online anormale, 31% incidente de accesibilitate și autenticitate și 11% acțiuni specifice

1. GSMA, „The Mobile Economy 2019”, pp.4-9, https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download, accesat în data de 12.04.2019.
2. CISCO, „Raportul Anual de Securitate Cibernetică, CISCO 2017”, Ianuarie 2017, Europe Headquarters, Cisco Systems International BV Amsterdam, The Netherlands, pp.10,93.

de administrare (*admin*, *root*), aceste 0.02% reprezentând amenințări reale.

Gândindu-ne la instrumentele preferate de atacatorii din mediul online în ziua de azi, sistemele malițioase de tip „*ransomware*", observăm că acestea sunt utilizate în atacurile sistemelor informatice ale companiilor la nivel global la fiecare 40 secunde, iar la fiecare ~15 secunde este atacat un utilizator individual. Aceste variante de ransomware se multiplică cu un factor de 4.3x în 2017 față de 2016, cu o rată de impact și de succes ridicată, de aproximativ 71%, pe când sistemele de securitate automatizate reușesc să respingă sau să izoleze un procent de aproximativ 29%, conform unuia din rapoartele globale privind atacurile de tip ransomware. Printre sectoarele vizate se numără Educația, IT&Telecomunicații, Media, Financiar, Guvernamental/Sector public/Apărare, Producție, Transport, Sănătate. Cu toate că în cazul a 4 din 5 companii, care au plătit răscumpărarea cerută, le-a fost oferit accesul la datele criptate, suma medie pretinsă în aceste cazuri se ridică la ~1077$ și de cele mai multe ori această „*taxă*" este achitată fără nici o garanție[1]. Ca dimensiune a fenomenului ransomware la nivel global, în 2017 avem trei mari variante de software malițios, care au făcut peste 700.000 victime: WanaCry (12 mai), ExPetr (27 iunie) și BadRabbit (octombrie)[2].

Deoarece perspectivele de obținere de bani prin utilizarea sistemelor de tipul ransomware sunt pe punctul de a fi eradicate sau cel puțin diminuate, din analiza evenimentelor și cercetărilor din acest mediu rezultă că următorul tip de instrument de atac va fi orientat în zona exploatării monedelor virtuale și a compromiterii bazelor de date cu conținut sensibil, precum datele cu caracter personal. Cu toate că au apărut cazuri izolate, acestea vor fi din ce în ce mai

1. Jonathan Crowe, „Must-Know Ransomware Statistics 2017, Stats & Trends", Iunie 2017, https://blog.barkly.com/ransomware-statistics-2017, accesat în data de 24.12.2017.
2. Kaspersky Lab, „Kaspersky Security Bulletin: Story of the year 2017", pp.5-8, https://cdn.securelist.com/files/2017/11/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf, accesat în data de 24.12.2017.

prezente, motivate fiind și de procentele în creștere privind viteza de transfer, utilizarea instrumentelor online și progresul tehnologic, precum și lacuna sau instabilitatea legislativă în plan național și internațional. Aceste tipuri de atac vor avea, din păcate, mai multe obiective ce vor fi atinse simultan, precum: mărirea rețelelor de tip *„botnet”*, utilizarea resurselor echipamentelor din aria tehnologiei informației și comunicațiilor conectate în rețeaua globală internet în vederea obținerii de resurse materiale care să ofere posibilitatea de anonimizare a posesorilor acestora, colectarea de date și informații în vederea valorificării acestora pe piața neagră, de regulă în scopuri malițioase sau ca simplă culegere de informații în vederea stocării acestora în sisteme de tip *„cloud”*, ce pot fi completate anonim și utilizate contra cost sau gratuit.

II.4.7. Aplicarea și implementarea politicilor de securitate asupra sistemelor informaționale în mediile virtuale

Deoarece aceste două arealuri - *real și virtual* - sunt în totalitate diferite, se impune o abordare unică și adaptată, contextuală și specifică. Putem evidenția acest lucru prin exemplificarea normativelor naționale în ceea ce privește protecția informației secrete de stat[1], unde legislația a fost concepută în contextul generării de documente predominant în format scris, pe hârtie, ulterior fiind actualizată și modificată pentru a fi relevantă contextului de securitate națională contemporan[2]. Față de acum 5-7 decenii, tehnologia a avansat și metodele, respectiv mijloacele prin care informația a căpătat o formă utilizabilă sunt azi prezente în cel puțin două forme, în format letric - *pe suport fizic* - și în format digital - *pe diverși suporți optici, magnetici, materiale semiconductoare*. Totuși, fundamental modalitatea de protejare și securizare a informației este aceeași, fiind doar actualizată

1. Legea nr. 182 din 12 aprilie 2002, *privind protecţia informaţiilor clasificate.*
2. Hotărâre de Guvern nr. 585 din 13 iunie 2002 *pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România.*

și completată de noi reglementări de ordin procedural. În contextul contemporan este obligatorie demararea și finalizarea unui proces de acreditare a mijlocului tehnic cu ajutorul căruia această informație este prelucrată.

Pentru clarificarea celor susținute, perspectivele propuse argumentează expunerea, cel puțin la nivel empiric, componentelor ce alcătuiesc esența a ceea ce conceptul de securitate națională tradițională oferă în raport cu provocările externe, unde identificăm un număr de patru concepte:

A. *Securitatea națională,* care include pe lângă securitatea intra-frontalieră și amenințări externe (oricare ar fi acelea) care necesită măsuri de protecție pentru conservarea integrității teritoriale și menținerea principiilor de funcționare ale statului de drept.
B. *Răspunsul*, care face referire la implicațiile reactive ale guvernului la astfel de amenințări:
   - Descurajarea: actul de limitare sau prevenire a unui conflict;
   - Apărare: actul de protejare a valorilor sau de întrerupere a conflictelor, chiar și prin metode și tehnici ofensive;
   - Costul conflictului: actul de contracarare a celeilalte puteri;
   - Conformare: acțiune inexistentă ca formă politică.
C. *Echilibrul puterii* reprezintă o necesitatea de dezvoltare a fiecărei țări:
   - Tehnologic;
   - Economic;
   - Militar;

Politicile orientate spre obținerea și păstrarea unui echilibru al puterii sunt necesare pentru a proteja valorile statelor în fața atacurilor din partea unor vecini cu agende ascunse sau din partea unor state

puternice, deoarece conflictele apar din mici neînțelegeri, cu excepția cazurilor în care există dorința unui stat de a cuceri un alt stat[1].

D. *Coaliția statelor* include o alianță a statelor pentru cooperare în cazul în care o țară atacă orice țară din coaliție, conform ideologiei supranaționalismului. În acest caz acordul dintre state și uniune ori coaliție trebuie să fie specific. Analiza permanentă a zonei de securitate va duce la identificarea amenințărilor în zonă, fie că este vorba de un conflict incipient sau de unul militar.

Totodată, acordul implică interesul național al fiecărei țări, fără a se leza interesul comun al țărilor membre. În cazul în care există o incompatibilitate între interesele statului și interesul comun, aceste acorduri se pot rezilia în orice moment.

Desigur, în contextul prezentei teze, atenția cade pe analiza conceptului de *„securitate națională"*, unde suntem datori să subliniem faptul că acesta este interdependent cu celelalte elemente *Răspunsul*, *Echilibrul Puterii* și *Coaliția statelor*. Motivația este una complexă, dar ușor de conceptualizat, atât în context realist cât și supranaționalist, un stat trebuie să își păstreze suveranitatea. Și cum poate realiza acest lucru dacă nu prin conceperea unui sistem perfect adaptat din punct de vedere diplomatic în procesul de păstrare a echilibrului puterii, în mediul intern al statului, dar și în cel extern - în contextul relațiilor internaționale. Acest act este desigur raportat la orice formă de asociere sau afiliere pe care acesta o are într-o coaliție internațională, identificat până și într-o poziție nefavorabilă, de conflict, unde este dator în a răspunde provocărilor pentru instaurarea unui echilibru a statului de drept.

1. Georgiana Roxana Muscu, „Lipsa exercitării suveranităţii ca un risc de vulnerabilitate pentru securitatea internaţională (*Cazul Ucrainei*)" în *Conferinţa Ştiinţifică Internaţională „Strategii XII - Complexitatea și Dinamismul Mediului de Securitate"*, Vol.1, , Edit. Universității Naționale de Apărare „Carol I", București, 2015, pp.8-9.

În cazul României, dacă vorbim de securitate națională, avem cel puțin două perspective de tratat. Prima este cea referitoare la Strategia de Apărare Națională, care rezonează profund cu „*Parteneriatul Strategic România - Statele Unite ale Americii*", apartenența și afilierea la NATO și UE, elemente care reprezintă fundamental temelia politicii externe românești. Apărarea și securitatea României, indiferent de dimensiunea și sectorul specific, este raportată și aliniată definitoriu la relația România - UE - NATO.[1]

În această ordine de idei, este necesar să subliniem poziția deținută de România în contextul de securitate local și global. Fiind o țară membră NATO începând cu 2004, a fost persuasiv îndemnată spre o participare activă PESCO și spre alocarea unui procent minim de 2.5% din PIB pentru Apărare[2]. Cu toate acestea, MApN a cheltuit în 2017 un procent de 1,81% din suma alocată, iar în 2018 un procent de 1,89%. România este vulnerabilă și datorită poziționării geografice într-o regiune cu un grad ridicat de concurență și competiție geopolitică între Occident și Rusia, vulnerabilitatea fiind crescută și de decizia luată - prin parteneriat strategic România-SUA – în 2013 de a găzdui părți din rețeaua de apărare anti-rachetă NATO. Acest fapt a dus la creșterea indignării Rusiei și a atras o atenție și un interes activ, neprielnic siguranței naționale din România. Alianțele încheiate de România în ultimii ani au adus-o într-o poziție definitorie, devenind un stat aflat sub protecția unor forțe supranaționale și nu doar vulnerabilă, ci și dependentă de protecția acestora, căutând în permanență să obțină asigurări din partea SUA și NATO cu privire la

1. Radu-Sebastian Ungureanu, Radu-Alexandru Cucută, „Europenization as a hegemonic project: Eu influence in approaching the security issues in the Balkans", în *New Challenges to the Balkan Security - Thematic Collective Book*, Vol.3, , Edit. Ivis, Veliko Târnovo, 2016, p.169.
2. Robert Lupitu, „Secretarul general al NATO atrage atenția privind alocarea a 2% din PIB pentru Apărare de către România: Sper că veți reuși să astupați acest gol", 31.01.2019, https://www.caleaeuropeana.ro/secretarul-general-al-nato-atrage-atentia-privind-alocarea-a-2-din-pib-pentru-aparare-de-catre-romania-sper-ca-veti-reusi-sa-astupati-acest-gol/, accesat în data de 12.08.2019.

protecția pe flancul estic, în mod special în zona Mării Negre. În ceea ce privește îndeplinirea atributului de stat membru al UE, NATO și ONU, România are parteneri strategici de securitate în state europene precum Germania, Franța și Anglia.

România favorizează vizibil și puternic cooperarea pe problematici de securitate națională în prim plan cu Washingtonul și apoi cu UE. Scepticismul României cu privire la garanțiile de securitate europene, datorită experiențelor sale din secolul XX, face ca acestea să fie privite de multe ori cu precauție. Cooperarea în domeniul securității și apărării în UE are o tendință ineficientă, dată de o competiție asupra resurselor de securitate între UE și NATO, ceea ce pune în pericol implicarea SUA în procesul de securitate națională a statelor membre și desigur de securitate europeană. Sentimentul general al României în ceea ce privește unele aspecte ale aderării la UE și ale integrării europene este împărțit, evidențiind în egală măsură efectele pozitive și cele negative asupra securității naționale, motiv pentru care și gradul de încredere al românilor în UE este ponderat - *„60% dintre români au o imagine pozitivă despre UE, față de 45% media europeană”*[1]. În consecință, România are o implicare limitată în PESCO, motivația principală a aderării a fost alinierea cu partenerii săi principali europeni, preluând și ducând la bun sfârșit cu rezultate[2] remarcabile președinția UE în 2019[3].

1. Comisia Europeană, „Eurobarometru de primăvară 2019: 60% dintre români au o imagine pozitivă despre UE, față de 45% media europeană”, 05.08.2019, https://ec.europa.eu/romania/news/20190805_eurobarometru_primavara_ro, accesat în data de 12.08.2019.
2. ”Președinția României la Consiliul Uniunii Europene, Coeziunea, o valoare comună europeană” https://www.romania2019.eu/wp-content/uploads/2017/11/Brosura-200x210-bilant-RO.pdf, accesat în data de 12.08.2019.
3. Guvernul României, „Prezentarea bilanțului rezultatelor obținute de Președinția României la Consiliul Uniunii Europene în primele 100 de zile de mandat, de către prim-ministrul Viorica Dăncilă”, 17.04.2019, http://gov.ro/ro/stiri/prezentarea-bilantului-rezultatelor-obtinute-de-pre-edintia-romaniei-la-consiliul-uniunii-europene-in-primele-100-de-zile-de-mandat-de-catre-prim-ministrul-viorica-dancila&page=3, accesat în data de 12.08.2019.

Indiferent de voința noastră, informațiile noastre sunt prelucrate în acest vast ocean de date, care nu se rezumă numai la internet, ci la toate rețelele - intranet - care îl compun sau cu care acesta este interconectat. Adesea se transmit știri mai puțin verificate, prin care se comunică capacități de securizare a datelor și informațiilor din partea organizațiilor ce vehiculează sau gestionează aceste date, care informează cu privire la securizarea acestora cu un procentaj de până la 100%. De menționat este faptul că în sectorul securității informației nu există acest procent nerealist de securizare, indiferent de forma pe care informația o are. Evident este faptul că informația, care stă la baza capacității de decizie politică, economică, militară și nu numai, trebuie tratată ca atare. Aceeași informație poate avea valori diferite în fiecare perioadă de viață a acesteia, acesta fiind și motivul pentru care s-a normat cu un număr exact de ani, specifici, păstrarea fiecărui document din clase de securitate. Dintotdeauna au existat politici de securizare și protecție a informației, acestea evoluând pe măsură ce sursele de generare a insecurității și-au făcut simțită prezența. Un sector, din păcate foarte activ în zilele noastre, este cel al comerțului informației pe piața neagră, sector care se regăsește într-o diversitate de rețele, precum și pe controversatul „*DarkWeb*".

Evenimentele, incidentele și breșele de securitate pot fi de două feluri: neintenționate și intenționate, dar procesul în care este prelucrat „produsul" mult râvnit de către inițiatorii sau generatorii acestor situații de insecuritate este obligatoriu reglementat într-un context aplicabil și funcțional. În fundamentarea acestei afirmații, trebuie să aducă în prim plan procesul și să identifice modalitatea de aplicare corectă a elementelor care conceptual formează sistemul specific de protejare a informației în aceste două mari arealuri, real si cibernetic.

Identificăm o organigramă care relevă strânsa relație de interdependență dintre procesele și elementele constitutive în vederea atingerii obiectivelor organizațiilor. Putem afirma că orice organizație ar trebui să aibă puse în aplicare, cu maximă seriozitate și consecvență,

ghiduri dedicate sectorului operațional. Desigur, aceste ghiduri sunt generate de procedurile specifice, care trebuie să fie conforme cu standardele aplicabile sectorului pentru care sunt elaborate, acestea fiind elemente operaționale și definitorii implementării proceselor de securitate pas cu pas, în conținutul cărora se pot regăsi instrucțiuni de proces și formulare necesare evaluării permanente a nivelului de securitate dat de proceduri.

Puntea de legătură între zona operațională și cea executivă este dată de nevoia de participare activă a celor două la implementarea standardelor interne sau internaționale special concepute pentru sectorul care necesită acoperirea unor carențe de securitate. Standardele sunt elemente necesare guvernării acestui sector de implementare a măsurilor de securitate utile, deoarece acestea sunt normativele care garantează prin aplicare împlinirea cerințelor de securitate, de monitorizare și control, pentru un management mai bun al organizației.

Acest bun management al organizației are un singur scop, anume identificarea de către conducerea organizației a celei mai bune soluții, în vederea atingerii obiectivelor organizației. Aceste obiective stau la baza elaborării tuturor politicilor care, desigur, trebuie să fie conforme cu legislația națională și internațională. Aceste politici trebuie să aibă o dublă aplicabilitate, în primul rând din perspectiva legală, prin conformarea la legislație, dar și din perspectiva operațională și executivă, marcată prin gestionarea resurselor și progresului organizației. Buna guvernanță, în acest context, este dată de măsura de aplicare a politicilor și de nivelul de securizare a informației, context care trebuie păstrat în balanța producție/securitate, fiind în permanență testată de nevoia de echilibrare conform intereselor organizației, indiferent de mediul în care aceasta activează și își desfășoară activitatea.

II.5. Teoria schimbărilor

Teoria schimbărilor marchează, din punct de vedere filosofic[1], transformările fundamentale în fenomenul de distribuție a puterii între națiuni, fapt care a redirecționat atenția spre aria de cercetare a relațiilor internaționale (IR), asupra percepției și înțelegerii schimbărilor și tranzițiilor de putere. În sectorul cibernetic, această teorie are o aplicabilitate pe un areal mult mai vast decât în sectorul managementului resurselor sau cel al relațiilor internaționale. *Teoria Schimbării* este, în esență, o descriere aprofundată și o ilustrare aproape plastică a motivului și a modului prin care o schimbare dorită sau necesară este prognozată într-un anumit context. În contextul sectorului cibernetic contemporan, această teorie preia aspectul elementului declanșator, tensionat de altfel de viteza evoluției tehnologice și a diversității modelelor de aplicabilitate. Se concentrează în special pe cartografierea și evidențierea nevoii de a completa locurile identificate a fi lacunare; analizează și evidențiază diferența dintre obiectivele și scopul final al securizării spațiului cibernetic, dar și pe metodele care sunt necesare a fi aplicate ori cercetate pentru a ajunge acolo, de aici rezultând un „deviz" al intervențiilor și activităților ce vor deveni condiții imperios necesare atingerii efectului scontat.

În aceste condiții, legătura dintre activități, intervenții și obiective este pe deplin înțeleasă. Așadar, avem o strategie prin care ne putem evalua poziția actuală în raport cu condiția precedentă pentru un progres incontestabil pe termen lung, ori până la atingerea scopului dorit (*în egală măsură tradițional și formal*). Dintre domeniile extern și intern, dintre secret și nesecret, dintre strategic și tactic sunt tot mai difuze, fiind estompate suplimentar de apariția noilor actori non statali (*grupări teroriste sau de criminalitate organizată, organizații*

1. Aseema Sinha, „Building a Theory of Change in International Relations: Pathways of Disruptive and Incremental Change in World Politics", în *International Studies Review*, Vol. 20, Nr. 2, Oxford University Press, Oxford, 2018, pp.195–203.

neguvernamentale sau companii private, alte entități difuze, fără sediu și fără doctrină) care acționează cu o viteză tot mai mare dincolo de granițele administrative.

Un studiu axat pe identificarea factorilor care au dus la această nevoie a schimbării de paradigmă a securității cibernetice poate fi pe deplin înțeleasă în condițiile în care se identifică lipsa de congruență între legislația și practica din toate domeniile de activitate în plan național și internațional. Desigur, pot aminti sumar câțiva factori generali, precum schimbările de regimuri politice, acțiunile asupra sistemului economic și bugetar național, progresul tehnologic urmat de deschiderea noilor arealuri cu perspective de dezvoltare a societății civile, dar și a sectorului privat, încercarea continuă de militarizare a spațiului virtual, multitudinea de reforme instituționale.

Drept dovadă, bazat pe analiza statistică a criminologiei cibernetice în plan internațional din ultimii ani și pe nevoia de schimbare, statele membre ale UE au agreat, în cursul lunii iunie 2017, să elaboreze un raport și ulterior un comunicat diplomatic al activităților cibernetice malițioase. Acest demers apare în urma activităților rău intenționate identificate în spațiul cibernetic al UE raportate la primele șase luni ale anului 2017 și a istoricului la nivel global sesizat de statele partenere în proiectele de monitorizare a arealului cibernetic.

Realitatea este că spațiul cibernetic vine în sprijinul tuturor sectoarelor societății cu oportunități semnificative, dar în același timp aduce în prim plan noi provocări pentru acțiunea externă a UE. Există un grad exprimat de îngrijorare privind capacitatea și disponibilitatea actorilor statali și nestatali de a-și atinge obiectivele cu ajutorul unor măsuri, tehnici și metode cibernetice malițioase. Acest tip de activități sunt constituite adesea în acte ilicite evidențiate și expuse de dreptul internațional și european, aducând în prim plan nevoia unui răspuns comun la nivelul statelor membre UE. Se reiterează statelor membre UE că, prin prin calitatea lor realistă de stat suveran și în aceeași măsură de aliat și stat membru al unei comunități globale,

nu trebuie să permită într-un mod voit ca spațiul lor geografic ori cibernetic să devină un teatru de operațiuni pentru înfăptuirea actelor ilicite și de terorism la nivel european, internațional și global. Cadrul diplomatic al UE face parte, conceptual, din arsenalul de instrumente diplomatice. Diplomația cibernetică și instrumentarul diplomației digitale, care își aduc un aport aparte la preîntâmpinarea și atenuarea evenimentelor diplomatice sensibile și a conflictelor, a atenuării amenințărilor de securitatea cibernetică, își aduc aportul direct și la stabilitatea geopolitică regională și globală. Acest nou cadru cu siguranță va veni în ajutorul și completarea nevoilor de cooperare în contextul relațiilor internaționale. Cu certitudine, acest cadru va facilita diminuarea riscurilor de amenințare pe termen scurt și va descuraja atitudinea agresivă a unor state, altele decât cele aliate pe termen lung. Feedbackul sectorului diplomatic al UE la activitățile ostile din mediul cibernetic se va raporta necondiționat la măsurile de politică externă și de securitate comune ale UE. Răspunsul diplomatic al UE la aceste tipuri de atacuri directe sau indirecte orientate spre suveranitatea statelor membre sau a structurilor organizaționale supranaționale ale UE este obligatoriu proporțional cu analiza de impact generată în urma analizei elementelor constitutive ale atacului precum: domeniu vizat, magnitudinea, durata, complexitatea atacului, intensitatea și impactul evenimentului de securitate cibernetic. „*UE își reafirmă angajamentul față de soluționarea diferendelor internaționale din spațiul cibernetic prin mijloace pașnice. În acest context, toate eforturile diplomatice ale UE ar trebui, cu titlu prioritar, să vizeze promovarea securității și a stabilității în spațiul cibernetic prin intensificarea cooperării internaționale și reducerea riscului de percepție eronată, de escaladare și de conflict care ar putea apărea în urma incidentelor din domeniul TIC*”[1].

1. Consiliul Europei, Comunicat din partea Secretariatului General al Consiliului, Bruxelles, 2017, p.4, „Atacuri cibernetice: Țările UE sunt dispuse să aplice sancțiuni ca parte a măsurilor sale pentru diplomație cibernetică”, http://www.caleaeuropeana.ro/atacuri-cibernetice-tarile-ue-sunt-dispuse-sa-aplice-sanctiuni-ca-parte-a-masurilor-sale-pentru-diplomatie-cibernetica/, accesat în data de 19.06.2017.

Lunile mai-iunie 2017 pot fi considerate ca fiind luni cu o activitate cibernetică malițioasă cu un impact major la nivel național. Atacuri cibernetice precum WannaCry au periclitat funcționarea în limite normale și uneori chiar minime a *„Sistemului Naţional britanic de Sănătate"* în luna mai[1], iar în luna iunie reprezentanții University College din Londra au avertizat personalul şi studenții în legătură cu riscul de pierdere a datelor şi de *„perturbări substanțiale"*. University College London (UCL) este un *„Centru de Excelență în Cercetare din Domeniul Securității Cibernetice"*, un statut acordat de serviciul de informații şi monitorizare GCHQ, aceasta aflându-se în top 10 universități din lume[2]. Aceste atacuri au avut replici, fiind atacate şi alte organizații din întreaga lume. Putem identifica acest nou areal cibernetic, de care într-o oarecare măsură aparținem, ca teatru de operațiuni mixt, deoarece forțele implicate aici la diferite nivele de activitate sunt din sectoare precum cele publice, guvernamentale, militare, paramilitare, civile și desigur anonime. Lipsa de congruență între actorii spațiului cibernetic duce la apariția de fragmente distructive, precum organizații ce duc o lupta de „gherilă cibernetică", în care grupuri mici de partizani conduși ideologic se împotrivesc societății civile prin mijloace oferite de sectorul cibernetic. Forțele de menținere a securității își fac apariția aproape de fiecare dată, dar de cele mai multe ori acest lucru se întâmplă prea târziu. Teoria schimbărilor în sectorul cibernetic, deși este cunoscută, nu este aplicată, preferându-se respectarea orbească a cutumelor și a legilor învechite sau permisive din cauza ambiguității cu care au fost întocmite.

Astfel, teoria schimbării este un proces riguros, dar participativ, prin care grupurile și părțile interesate, printr-un proces de planificare, își argumentează obiectivele pe termen lung și își identifică

1. Chris Foxx, „NHS cyber-attack: GPs and hospitals hit by ransomware", http://www.bbc.com/news/health-39899646, accesat în data de 13.05.2017.
2. Sean Coughlan, „Top university under ‚ransomware' cyber-attack", http://www.bbc.com/news/education-40288548, accesat în data de 15.06.2017.

condițiile pe care le consideră necesare pentru îndeplinirea acestor obiective. Aceste condiții sunt generate ca rezultate dorite, aranjate grafic într-un cadru cauzal chiar algoritmic, ca mai apoi, în baza unei hărți relaționale, să se monitorizeze pas cu pas procesul de implementare, iar în baza unui sistem de răspuns și audit permanent să fie luate decizii pentru împlinirea obiectivelor la cele mai înalte standarde. Conform gradului de satisfacție al grupului de lucru în ceea ce privește atingerea obiectivelor propuse, respectiv conform teoriei schimbării, se vor face analize la nivel micro pentru identificarea unor noi obiective sau pentru identificarea unor noi căi de a atinge obiectivele programate. Astfel,putem înțelege rolul progresului tehnologic și al produselor apărute o dată cu această revoluție tehnologică. Este suficient să reflectăm asupra deciziilor luate de factorul de decizie de la nivelul oricărei organizații contemporane în ceea ce privește atingerea unui obiectiv, oricare ar fi acela. Se poate observa cu ușurință că digitalizarea și utilizarea tehnologiilor de comunicații voce-date a făcut mai mult decât să sporească producția sau progresul organizației pentru atingerea obiectivelor propuse. În foarte multe cazuri, organizațiile, bazându-se pe teoria schimbării, au adaptat strategii, care au dus la o reconceptualizare a întregului sistem de afaceri. Domeniul cibernetic a ajuns să fie o componentă fără de care organizațiile contemporane, indiferent de sectorul acestora de activitate, nu pot progresa, ci pot cel mult exista.[1]

Concluzii preliminare

Ca urmare a cunoașterii elementelor ce compun managementul informațiilor vehiculate în arealul cibernetic și a înțelegerii rolului

1. Anandhi Bharadwaj, Omar A. El Sawy, Paul A. Pavlou, N. Venkatraman, „Digital Business Strategy: Toward a Next Generation Of Insights", în *MIS Quarterly*, Vol. 37 Nr. 2, Edit. MISRC, Minnesota, 2013. pp.474-476.

managementului riscului în organizațiile contemporane, putem să evaluăm impactul utilizării informației și în același timp să analizăm în profunzime sursele generatoare de insecuritate la adresa informației, pentru o minimizare a nivelului de risc. După cum reiese din prezentul capitol, unul dintre cei mai importanți factori care pot influența într-o mare măsură atât pozitiv cât și negativ sistemele, procesele și mecanismele sistemului de management a informației electronice sunt oamenii. Acesta este factorul declanșator al majorității incidentelor de securitate și infracțiunilor informatice. Înțelegem așadar că pregătirea continuă în domeniul protecției informației și apărării împotriva factorilor de risc este de necontestat printre primele nevoi ale organizației, dar și ale individului. Vulnerabilitatea nu este dată doar de lipsa unor măsuri protective ale organizației, factorul uman - care este și cel mai valoros bun al organizației - este cel al cărui nivel de cunoștințe și grad de înțelegere a conceptului de securitate cibernetică trebuie cultivat și crescut. Calitatea și existența unui cult al elitelor de securitate a informației în orice organizație este imperios necesară pentru a acoperi cel de-al doilea nivel de nevoie fundamentală a omului, siguranța și securitatea, aceasta fiind în ziua de azi, în mare parte, reprezentată de arealul cibernetic. Crearea de relații interumane prin comunicare, consult și colaborare între zona de management și cea de execuție în organizație crește nivelul de încredere al sistemului de securitate. Neacoperirea nevoilor logistice primare ale sistemului de securitate (*echipamente, audit, management, cercetare, experți în studii de securitate și ingineri de securitate*) duce negreșit la un colaps informațional. Deși relativ recentă (< 50 ani), punctarea managementului sau guvernării prin risc, care este un nou cadru de analiză, trebuie să facă parte din orice proiect managerial. Identificarea unui portofoliu de management al riscului optim presupune selectarea unei suite de strategii, în funcție de aplicarea sistematică a identificării şi analizei riscurilor. Datorită permanentelor evoluții ale lumii cibernetice, pentru o mai bună guvernare este

nevoie de o permanentă actualizare a cadrului legal, atât național cât și internațional. O propunere pertinentă ar fi crearea unei comunități globale de securitate și analiză de risc, care să colaboreze în permanență în spectrul ariilor cibernetice, virtuale, electronice, informaționale și administrarea acesteia de către un management elitist cu viziune în sectorul cibernetic.

Necesitatea ridicată de gestionare a informației pentru obținerea celei mai bune decizii, cu atât mai mult în contextul securității naționale, nu lasă loc pentru erori. Totuși, fie că vorbim de națiuni, federații, uniuni sau alte forme supranaționale, trebuie să ținem cont că orice stat are nevoie să fie suveran sau suveran în cadrul alianței. Resursa primară cu care se lucrează, deocamdată, este cea umană, motiv pentru care informația poate fi ușor alterată (direct sau indirect). Datorată limitărilor resursei umane, din lipsa capacității de procesare umană a informațiilor, s-au dezvoltat noi sisteme inteligente de prelucrare a acestora. Astfel, regăsim în această sferă de interes și cercetare:

- automatisme și mecanisme bazate pe inteligența artificială cu capacități de procesare extraordinare, cărora le lipsește doar rațiunea și emoția umană;
- sisteme de învățare automată bazată pe procese anterioare (succes/eșec) numite „*machine learning*[12]" și inteligență artificială;
- sisteme consacrate care, prin funcțiile lor de procesare și predicție, pot oferi cele mai bune rezultate pentru managementul și progresul organizațional, cuantificate mereu în resurse financiare.

---

1. Machine learning: *termen în limba engleză tradus în limba română ca sistem informatic de inteligență artificială pentru învățare automată.*
2. Léon Bottou, Frank E. Curtis, Jorge Nocedal, „Optimization Methods for Large-Scale Machine Learning", în *SIAM Review*, Vol. 60, Nr. 2, 2018, pp. 223-311.

Aceste sisteme de competitivitate prin informație, sisteme informatice de procesare prin recunoaștere, localizare, extragere, analizare a informațiilor disponibile - structurate sau nestructurate - într-o organizație și raportarea acestora către decident sau sistemele informatice ce au ca obiectiv furnizarea celui mai bun suport în luarea deciziilor în sectorul de afaceri (BI: *Business Intelligence*), aduc valoare sistemului informațional în orice organizație. Companiile pot lua decizii care să se materializeze prin reducerea de costuri sau reducerea timpului de execuție ori utilizare a unor resurse - acestea se regăsesc de regulă în zone cu pierderi nejustificate. Într-o organizație, aceste instrumente sunt create pentru a putea administra cât mai eficient informația și activitățile pe care aceasta le influențează, anume cele operaționale și strategice, aducându-le la o funcționalitate optimă conform obiectivelor organizației.

Necesitățile informaționale ale unei entități moderne reflectă cel mai bine obiectivul cercetării noastre, deoarece soluționarea provocărilor cu care este confruntată organizația în zilele noastre reprezintă subiectul pe care îl voi aprofunda în lucrarea de față.

Politicile de securitate capătă forme diferite în funcție de *„bunul"* care are nevoie de a fi securizat, valoarea efectivă a acestuia, *„puterea de cumpărare"*, proprietarul și beneficiarul informației, interesele și efectele diseminării acesteia în anumite medii de interes, menționând că de obicei efectele se măsoară în dimensiuni economice, financiare sau dimensiuni ale puterii. Cu toate acestea, înțelegem că managementul informațiilor în orice organizație, indiferent de mediul și sectorul de activitate sau de dimensiunea acesteia, este strâns corelat cu clasificarea acesteia, riscul pe care este dispusă să și-l asume și vulnerabilitățile care pot compromite integritatea acesteia.

Elementele de noutate apărute în acest capitol sunt date de expunerea nevoii de conceptualizare a unui nou cadru de analiză și guvernare a resurselor materiale și cibernetice pentru o bună guvernanță a spațiului cibernetic cu ajutorul elitelor formate pe sectoarele de nișă

noi apărute. Pentru a întări această viziune, consider aplicabilă teoria schimbării în primul rând în zona de cercetare a relațiilor internaționale raportată la acest nou areal virtual și a cărui efecte în zona de guvernanță a sectorului informațional nu pot fi ignorate. Teoria schimbării este un element cheie în progresul tuturor științelor, motiv pentru care aceasta trebuie adaptată și noului context informațional digital contemporan. Teoria schimbării și arealul cibernetic sunt două dintre cele mai importante elemente constitutive ale noii ere - fie că este vorba de cuantică sau ceva mai mult de atât.

Capitolul III.
Guvernanța spațiului virtual în concepția realismului și supranaționalismului

III. 1. Implicațiile arealului cibernetic asupra relațiilor internaționale în viziunea teoriilor realismului.

În actualul context geopolitic, influențat de lipsa granițelor tangibile, realismul este redefinit în extenso prin faptul că nu există până în acest moment o autoritate centrală recunoscută unanim care să aibă rolul de regularizare a raporturilor dintre state asupra influenței în arealul cibernetic. Totuși, pentru a fi precaut cu privire la afirmații de o asemenea magnitudine, consider că este necesară o interpretare a acestuia în care să se aibă în vedere influențele progresului și inovației

tehnologiei contemporane, respectiv paradigma securității cibernetice în contextul guvernării la nivel național și federal ori chiar global.

Pentru a aprofunda implicațiile evenimentelor și a acțiunilor din arealul cibernetic asupra relațiilor internaționale în viziunea primei teorii a relațiilor internaționale - realismul, ce reprezintă o puternică școală de gândire - consider că este necesară înțelegerea conceptului de realism ca termen definitoriu al teoriilor care îl susțin. Realismul este perceput ca fiind încercarea de transformare a regulilor practicii diplomatice (secolul al XIX-lea) în legi științifice în raport cu o știință socială dezvoltată cu mai intens în Statele Unite ale Americii[1].

Așadar, cunoscând faptul că *relațiile internaționale* reprezintă studiul inductiv al interacțiunilor și raportărilor actorilor statali la cei non-statali, considerăm *realismul politic* ca fiind una dintre principalele teorii care încearcă să explice relațiile dintre dintre state. În încercarea de a explica relațiile internaționale dintre state în termeni de putere, realismul politic aduce argumente concretizate și adaptate la capacitatea statelor de autoguvernare.

III.3.1. Raportul forțelor din mediul internațional în contextul realismului

În contextul relațiilor internaționale, termenul de putere este în principiu reprezentat de capacitatea unui stat de a convinge un alt stat în luarea de decizii pe care în mod obișnuit și natural acesta nu ar lua-o, sau capacitatea unui stat de a opri acțiunile interne sau externe ale unui alt stat, acțiuni pe care în mod natural acesta dorește să le facă. Un aspect definitoriu în acest caz este puterea „impusă" a unor state asupra deciziilor altor state indiferent de influența și presiunea internă a statului asupra căruia se manifestă puterea politică internațională. Pentru a ilustra conceptul descris, voi oferi un exemplu.

1. Guzzini Stefano, *Realism şi Relaţii Internaţionale – Povestea fără sfârșit a unei morți anunțate: realismul în relațiile internaționale și în economia politică internațională* (trad. Diana Istrăţescu), Edit. Institutul European, Iaşi, 2000, p.40.

Să presupunem că un anumit oraș O, care, fiind în curs de dezvoltare industrială, este împiedicat în procesul evolutiv de legile ambigue ale statului X de pe teritoriul căruia se află. Industria acestui stat X, din lipsa unei guvernanțe elitiste, în timp, a fost aproape eradicată, rămânând pe piață doar micii producători. În acest context, administrația locală consideră că este necesară încheierea de parteneriate strategice cu organizații corporative internaționale. Acest proces este împiedicat de factori precum factorul de corupție, lipsa unei legislații coerente și aplicabile, lipsa cunoștințelor pe sectoarele de nișă ale industriei șamd. Unul dintre partenerii strategici ai acestui oraș are un capital de stat majoritar și implicit devine o situație de interes național, respectiv internațional, pentru statul Y. Totodată, acest stat Y este unul care își poate impune condițiile și pretențiile la nivel internațional, așadar creează un precedent prin „convingerea" statului X să ia măsuri favorabile parteneriatelor strategice între orașul O și organizațiile/corporațiile și piețele de desfacere de pe teritoriul statului Y.

Într-un mod evident, România, ca țară cu evidente nevoi privind securitatea, se află într-un context diplomatic sensibil față de țările cu care aliații săi nu sunt în cele mai bune relații. Din fericire, alianțele cu vecinii apropiați și îndepărtați pot asigura un grad ridicat de securitate, alianța fiind mai puternică decât potențialul risc adus de amenințările statelor adverse. Desigur, nimic nu este gratuit, așadar aliații României așteaptă o deschidere cât mai mare în ceea ce privește piețele interne și pretenția de a importa fără nici un fel de tarife, sau alte bariere comerciale, bunuri și servicii. În mod normal, acest lucru nu este neapărat favorabil sau necesar României, dar cetățenii se bucură de plaja largă de servicii și diversitatea de bunuri importate. Angajarea României în acțiunile strategice ale aliaților nu este favorabilă pe termen scurt, mediu sau lung.[1]

1. Iulian Fota, „Rusia cere SUA să distrugă rachetele de la Deveselu. Iulian Fota: Rusia pierdea teren. Trebuia să arunce o carte pe masă", https://www.digi24.ro/stiri/actualita-

Întrebarea este „*Ce face un stat puternic?*". Puterea în acest caz este dată de capacitatea de influență a unui stat asupra altuia sau asupra unui areal geografic, politic, cultural șamd. În context internațional, această capacitate se bazează pe caracteristicile tangibile și intangibile ale statului.

Caracteristicile tangibile ale statelor includ aspecte ca dimensiunea unui stat, geografia, resursele naturale, sectorul economic, sectorul militar, dezvoltarea tehnologică și populația.

Caracteristicile intangibile includ elemente precum voința și identitatea națională, sprijinul popular al guvernului și ideologia. Deși puterea militară nu este singura cale spre putere pe scena mondială, susținătorii curentului realismului tind să creadă că este cea mai importantă.

III.1.2. Școala de gândire realistă

Realismul ca școală de gândire promovează statul și valorile acestuia în relațiile internaționale. Statul, indiferent de forma de guvernare a acestuia, este actor principal, iar suma obiectivelor acestuia reprezintă rezultatul efortului de acaparare a puterii în toate planurile. Liantul pe baza căruia statele își construiesc o relație există pentru ca acestea să-şi promoveze interesele proprii atât în regiune cât și în extenso la nivel global. În concepția adepților teoriei realiste, anarhia este unul dintre elementele reprezentative ale statului. În acest context, analizele teoreticienilor care s-au aplecat spre studiul realismului susțin că, motivate de haosului din interiorul statului, elitele din sectorul politic pot gestiona crizele, drept urmare pot apăra suveranitatea și valorile statului. Ca urmare a acestei ipoteze, se dezvoltă ideea că statul care gestionează cel mai bine situațiile de criză va avea tendința de a domina statele din proximitate și relațiile cu statele mai îndepăr-

te/rusia-cere-sua-sa-distruga-rachetele-de-la-deveselu-iulian-fota-rusia-pierdea-teren-trebuia-sa-arunce-o-carte-pe-masa-1078462, accesat în data de 22.08.2020.

tate. Aceeași teoreticieni au oferit liderilor de stat conceptul *„rațiunii de stat"*[1], prin care se promovează ideea că un decident politic este îndreptățit și obligat să identifice și să aleagă decizia circumstanțială favorabilă statului în momente de criză, indiferent de repercusiunile acestei decizii în contextul relațiilor internaționale.

Drept urmare, un stat puternic este un stat a cărui conducere este rezilientă în fața crizelor și a presiunilor contextului geopolitic, așadar acestui stat îi sunt sporite șansele de a rezista și a răspunde eficient în cazul oricărui act ofensiv sau de subminare din partea altor state. În subsidiar, se consideră că o elită sau un stat puternic poate să depășească limitele diplomatice încălcând tratate, convenții sau alte forme de garantare a parteneriatelor internaționale *-folosind uneori forța militară* - doar pentru a-și atinge obiectivele cu repercusiuni sau represalii nesemnificative.

Școala de gândire realistă are la bază patru teorii diferite care o susțin:

A. **Realismul clasic** a cărui fondator a fost Tucidide și care susține conceptul naturii umane. Această teorie susține că elitele politice adesea sunt dominate de putere și influență, fiind astfel mai ușor ispitite în încălcarea legilor, nerespectarea drepturilor omului sau a codului etic și moral.

B. **Realismul istoric,** a cărui fondatori au fost Niccolò di Bernardo dei Machiavelli, Hans Joachim Morgenthau şi Edward Hallett *„Ted"* Carr, susține că atâta timp cât pe primul loc în luarea deciziei se regăsesc factorii de putere, principiile morale şi etice sunt clasate în plan secund de către conducătorii unui stat.

C. **Realismul modern** cunoscut ca **Realism structural**, este reprezentat în primă instanță de Jean Jacques Rousseau, iar mai târziu de Kenneth Neal Waltz. Aceștia mizează pe premisa că datorită factorilor destabilizatori, precum anarhia sau instabi-

1. Traducere din franceză: *raison d'etat*

litatea sistemului politic, pot apărea conflicte ușor scalabile, cu toate că nu întotdeauna actorii politici au intenții obscure sau negative.

D. **Realismul liberal** susține că toate statele puternice pot acționa în vederea prevenirii, medierii sau dizolvării unor conflicte, chiar dacă acestea au fost generate într-un context anarhic[1].

Conform teoriilor realismului, adepții școlii de gândire realiste ar putea fi considerați cinicii relațiilor internaționale[2], unii dintre aceștia lansând ipoteze despre lume precum:

√ Oamenii prin natura lor sunt catalogați ca fiind egoiști. Oamenii nu fac lucrurile în interes social sau de obște; oamenii fac lucruri pentru că acestea servesc un fel de nevoie egoistă care face parte din natura noastră umană[3].

√ Anarhismul stă la baza întregului sistem politic internațional. Este o lume perfidă unde cel mai puternic domină.[4]

√ Cei mai importanți actori din lume sunt statele, iar conflictul este starea naturală a relațiilor dintre state.[5]

√ Statele acționează în moduri raționale cu scopul de a-și servi propriile interese[6].

√ Singurul control al puterii unui stat este dat de un alt stat sau de un grup de state. În sistemul anarhist al relațiilor interna-

1. Matt Sleat, *Liberal Realism: A Realist Theory of Liberal Politics*. Manchester University Press, 2013.
2. Ciprian Nițu, *Cosmopolitismul-Către o nouă paradigmă în teoria politică*, Edit. Adenium, Iași, 2014,p.45.
3. Annette Freyberg-Inan, *What Moves Man: The Realist Theory of International Relations and Its Judgement of Human Nature*, State University of New York Press, Albany, SUA, 2004, pp.85-87.
4. Robert Powell, „Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate", în *International Organization*, Vol. 48, Nr. 2, The MIT Press, Massachusetts, 1994, pp. 313-344.
5. Cristopher Daase, „The English School", în *Theories of International Relations*, Edit. Routledge Taylor & Francis Group, Londra, 2014, pp.150-151.
6. Charles L. Glasser, „Realists as Optimists: Cooperation as Self-Help", în *The Perils of Anarchy: Contemporary Realism and International Security*, The MIT Press, Massachusetts, 1995, pp.336-340.

ționale, limita acțiunilor unui stat este infinită atât timp cât nu există o altă forță care să se opună.

- √ Moralitatea în sistemul internațional trebuie tratată cu scepticism; simțul moral în acest sector poate fi contraproductiv pentru o acțiune politică de succes. Scopul principal este dat de necesitatea de supraviețuire prin orice mijloace, expresia cea mai potrivită ar fi metodele justifică mijloacele și scopul scuză faptele[1].

Obiectivul cercetării nu stă în infirmarea sau confirmarea acestor teorii. În ceea ce privește România, în calitate de stat membru al UE, se dorește o înțelegere a mecanismului de guvernare a spațiului cibernetic din perspectiva securității naționale, prin înțelegerea aplicabilității teoriilor care stau la baza școlii de gândire realiste. Se pot identifica anumite corelări între tipul de guvernare al UE în raport cu statele membre și cu statele non membre, dar partenere. Totodată, se poate observa cum statele duc o luptă pentru a păstra un echilibru între a-și păstra suveranitatea într-o construcție federală și, în același timp, de a încerca o aliniere la obiectivele și viziunea comună.

Spre exemplu, în contextul realismului, suveranitatea poate fi reprezentată de elementele principale și necesare privind existența și funcționarea statului, elemente precum *teritoriul*, *populația* şi un *guvern* eficient. În prezent, înțelegerea suveranității în cele 193 de state membre din cadrul ONU pornește de la prioritizarea și protejarea acestor trei elemente în raport cu orice acțiune externă a statului[2]. În prezent sunt disputate două interpretări ale suveranității, anume *suveranitatea statală* și *suveranitatea naţională*.[3]

1. Diana T. Meyers, *Political Realism And International Morality: Ethics In The Nuclear Age, – Part One Morality and the International Order: Introduction to Part One*, Edit. Routledge Taylor & Francis Group, New York, SUA, 2019, pp.1-6.
2. Lista cu satatele membre ONU, „Member states", https://www.un.org/en/member-states/, accesat în data de 10.08.2019.
3. Georgiana Roxana Muscu, *op.cit.* p.8.

III.1.3. Echilibrul puterilor

Luând exemplu performerilor sportivi care posedă calități fizice pe care majoritatea persoanelor nu le au sau observând resursele intelectuale pe care geniile le au, putem înțelege de ce nu toate țările au capacitatea naturală de a deveni suficient de puternice pentru a rezista de unele singure sau pentru a domina în sectorul relațiilor internaționale.

Și în sectorul relațiilor internaționale există state sau actori non-statali care aduc în arena internațională potențiale riscuri la adresa securității naționale sau la adresa integrității alianțelor, aceștia mizează aproape de fiecare dată pe evidențierea raportului de forțe și de implicații aduse de valoarea lor pe „*piața*" relațiilor internaționale.

În aceste condiții, un stat care nu are resursele necesare pentru a se opune, poate să facă apel, conform susținătorilor curentului realismului, la principiul echilibrului puterilor. Acesta aduce în prim plan posibilitatea de a capacita resursele unei puterii sau a mai multor state care să echilibreze puterea unui stat sau a mai multor state, cu scopul de a se armoniza o stare de echilibru[1].

Dezvoltarea de tehnologii privind gestionarea informațiilor vehiculate în mediile virtuale și procesul de înarmare cibernetică a unui stat duce la o creștere a relevanței acestuia în context internațional în materie de furnizor de securitate. Acest lucru duce la o reevaluare a puterii și influenței unui stat în plan geopolitic și geostrategic. Puterea oferită unui stat de capacitarea cibernetică a acestuia în calitate de stat aliat poate schimba ușor echilibrul puterilor în cadrul alianței. Utilizarea arealului cibernetic în contextul de securitate internațional poate avea rezultate benefice pentru state și alianțe - *piața digitală unică, comunicarea de voce/date securizată în timp real, telemunca șamd* -, dar poate ajuta la destabilizarea economică și politică, vulnerabilizarea infrastructurilor critice, derularea de campanii de dezinformare

1. Cristopher Daase, *op.cit.,* p.151.

și propagandă în defavoarea statului și a cetățenilor acestuia, iar exemplele pot continua și pot ajunge până la cazuri de atingere a securității naționale prin lansarea și susținerea de atacuri cibernetice direcționate și coordonate.

Din această perspectivă a puterii reflectată de cursa înarmării și capacitării cibernetice militare, de intelligence sau e-guvernare, putem spune că echilibrul puterilor în plan internațional trebuie tratat precum este în prezent gestionată proliferarea înarmării nucleare sau a armelor neconvenționale.

III.1.4. Puterea cibernetică în contextul realismului contemporan

Puterea reprezintă un element definitoriu, esențial chiar, pentru realism, deoarece poate asigura independența și supraviețuirea statului într-un mediu autoguvernat și autosuficient.[1]

După cum afirmă Morgenthau, *„oricare ar fi ultimul scop al politicii internaționale, puterea este întotdeauna obiectivul imediat”*[2]. Adesea susținătorii realismului echivalează puterea cu o resursă esențială a statului, precum sunt resursele naturale, capacitatea industrială, forța militară și populația unui stat[3].

Puterea cibernetică este definită de Nye[4] ca fiind *„abilitatea de a obține rezultate scontate prin utilizarea resurselor sistemelor informaționale interconectate din sectorul cibernetic”*, iar potențialul acestui tip de putere de a transforma sau redefini conceptual, dar și practic relațiile internaționale, a devenit o dezbatere proeminentă la nivel global. Inexistența unei teorii privind puterea cibernetică în literatura realistă nu oprește realismul în a dezvolta un cadru de studiu larg în care să

1. John J.Mearsheimer, "Structural Realism", în *International Relations Theories:Discipline and Diversity*, Oxford University Press, Oxford, 2006, pp. 71–88.
2. Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace*, New York, Edit. Alfred A. Knopf, 1949, p.13, https://archive.org/details/in.ernet.dli.2015.74487/page/n35, accesat în data de 29.11.2018.
3. *Ibidem*, pp.80-108.
4. Joseph S. Nye, *The Future of Power,* Edit. Public Affairs, New York, 2011, p.123.

se genereze diverse ipoteze de distribuire a puterii între actori statali și non statali în sectorul virtual, precum și modul în care este tratat conflictul cibernetic din perspectiva realismului.

Pornind de la premisa realismului, care indică statul ca principalul actor în domeniul politic internațional și înțelegând și asumându-ne evoluția digitală și în general progresul tehnologic, printr-o analiză introspectă a realității suveranității statelor asupra arealurilor descoperite până în prezent, ajungem la o posibilă nevoie de a schimba paradigma statul este suveran prin puterea generată și gestionată de acesta. Acest uriaș progres tehnologic din ultimii 50 ani pune în discuție poziția actorului statal chiar și prin implicarea marilor actorilor non-statali care amenință dinamica și tendința tradițională de utilizare a puterii în context politic și nu numai[1]. Actorii non-statali sunt din ce în ce mai importanți în ceea ce privește gestionarea relațiilor internaționale. Conform teoriei distribuirii puterii a lui Nye[2], acest lucru este vizibil mai ales în domeniul cibernetic, unde diverși atacatori, grupuri de criminalitate organizată sau grupări teroriste profită de ușurința accesului la resursele spațiului cibernetic pentru a amenința și chiar atenta la vădita suveranitate a statului asupra unor zone ale acestui domeniu virtual. În același context de securitate națională, regională sau internațională, se regăsesc și firmele private sau firmele cu capital privat-public, rolul acestora fiind unul extrem de relevant și important, atât din perspectiva calității de generatori de securitate obținute de acestea, cât din cea a calității de surse de insecuritate prin vulnerabilitatea și riscurile la care se supun.

---

1. Eriksson Johan, Giampiero Giacomello, „The Information Revolution, Security, and International Relations: (IR) Relevant Theory?”, în *International Political Science Review*, Vol. 27, nr. 3, 2006, pp. 228–229, https://www.researchgate.net/publication/249743496_The_Information_Revolution_Security_and_International_Relations_IRRelevant_Theory, accesat în data de 03.12.2018.
2. Joseph S.Nye, „Soft Power”, în *Foreign Policy*, no.80, Edit. Washington Post, Washington, 1990, pp.160-161, https://www.wilsoncenter.org/sites/default/files/joseph_nye_soft_power_journal.pdf, accesat în data de 03.12.2018.

Ignoranța sau dezinteresul față de această problemă nu reprezintă o soluție, deoarece statele sunt deocamdată actori unici în problematica gestionării și stabilirii echilibrului în zona de conflict cibernetic. Actorii non-statali, crima organizată și terorismul cibernetic joacă un rol important, însă tacticile lor au fost, în general, total ineficiente sau, în unele cazuri, folosite ca acțiuni „paravan" pentru statele-națiune în încercarea acestora de a-și ascunde acțiunile[1]. Statele inteligente, corect guvernate și competitive pe „piața" relațiilor internaționale, rămân deocamdată cele mai bine poziționate în mobilizarea și instrumentarea unui ipotetic război cibernetic, puternic ancorate nu doar în resursele financiare sau resursa umană, cât și în politicile cu rezultate din sectoarele cercetării, inovării, dezvoltării și educației.

Pornind de la costurile necesare și relativ scăzute ale înarmării unui stat în domeniul războiului cibernetic, identificăm o altă schimbare de paradigmă a războiului. În acest al cincilea areal, intangibil și relativ ușor de accesat, statele mai slabe provoacă statele mai puternice, chiar prin dezvoltarea concentrată a capacităților digitale în spațiul virtual, totodată generând o forțată redistribuire a puterii, afectând puternic chiar întregul sistem global de securitate. Putem exemplifica prin sute de cazuri, dar consider direct relevante doar câteva, precum cazul complexității tacticilor cibernetice ale Iranului, care cu ajutorul elitei armatei iraniene, Garda Revoluționară Iraniană, a desfășurat un adevărat front de luptă cibernetic față de S.U.A.[2] sau cazul Coreei de Nord[3], care a pregătit mii de hackeri pentru a acționa

1. Valeriano Brandon, Ryan C. Maness., „Cyber War versus Cyber Realities: Cyber Conflict in the International System, New York", Edit. Oxford University Press, New York, 2015, pp.164-187, https://www.researchgate.net/publication/282792147_Cyber_War_versus_Cyber_Realities_Cyber_Conflict_in_the_International_System, accesat în data de 03.12.2018.
2. Jay Solomon, U.S. Detects Flurry of Iranian Hacking, „American officials say they believe cyberattacks tied to arrest in Tehran of Iranian-American businessman", 4 noiembrie 2015, https://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754, accesat în data de 03.12.2018.
3. Mulrine Anna, „How North Korea built up a cadre of code warriors prepared for cyberwar", 06.02.2015, https://www.csmonitor.com/World/Passcode/2015/0206/How-

în spațiul cibernetic la nivel global sau cazurile grupurilor APT (*en. Advanced Persistent Threat Groups*) care sunt de regulă finanțate de statele intrate în această cursă. Scopurile principale ale acestor grupări sunt de a încerca să culeagă date și informații în toate formele sale, dorind să saboteze operațiuni și să distrugă infrastructuri. Cert este că acestea acționează într-un interval de timp care se poate întinde de la câteva zile până la 4-5 ani asupra aceluiași obiectiv. Au capacitatea de a se readapta la formele de protecție apărute între ei și țintă, pe care le vor sparge sau ocoli cu perseverență atâta timp cât obiectivul este de interes. Pe portalul FireEye[1] apare un număr de aproximativ 38 de astfel de grupări din țări precum Coreea de Nord (APT38, APT37), Iran (APT34, APT3.3), Vietnam (APT32), China (APT30) și Rusia (APT29, APT28, APT19, APT18, APT17, APT16, APT12, APT10, APT3, APT1). În afară de cele deja expuse, sunt multe altele care își desfășoară activitatea sub observația atât a actorilor non-statali, cât și a statelor cu capacitate tehnologică avansată. Majoritatea atacurilor provenite din partea oricărei grupări (cu atât mai mult din partea celor finanțate de state) sunt atacuri complexe, inteligente. Doresc să aduc în prim plan APT1 sau Unitatea 61398, care a colectat ilegal și clandestin, sistematic sute de terabyte de date de la cel puțin 141 de organizații și totodată și-a demonstrat capacitatea și intenția de a fi operațional simultan asupra mai multor zeci de organizații. Din analizele asupra activității desfășurate de grup începând cu anul 2011, s-a constatat că acesta se concentrează pe compromiterea organizațiilor dintr-o gamă largă de industrii, aflate în țări vorbitoare de limba engleză. Dimensiunea infrastructurii APT1 este estimată de la zeci la sute de operatori umani. O deconspirare a operațiunilor acestei grupări a fost făcută de companii private din sectorul securității cibernetice, precum Mandiant, care au publicat o serie de

North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar, accesat în data de29.11.2018.

1. Advanced Persistent Threat Groups, „Who's who of cyber threat actors", https://www.fireeye.com/current-threats/apt-groups.html, accesat în data de 29.11.2018.

dovezi privitoare la activitățile Armatei Populare de Eliberare (APE) Unitatea 61398, care făcuseră parte în trecut din Biroul al doilea al Departamentului de Stat Major. Acesta era format din mii de militari cu abilități digitale, despre care se crede că erau specializați în operațiunile de compromitere a rețelelor informatice și compromiterea sistemelor informatice din mai multe industrii cu importanță strategică și economică[1].

Desigur, existența acestor unități militare de profil este cunoscută, mai ales în comunitățile de informații din spectrul relațiilor internaționale. Unele dintre acestea sunt promovate chiar de statele sub egida cărora acționează, acestea fiind afiliate statelor 100%. O astfel de unitate este Unitatea 8200 (*Yehida Shmoneh-Matayim*) subordonată Aman, care la evenimentul anual CyberTech2017[2], desfășurat în Tel Aviv (Israel), a fost subtil edificată de Prim-ministrul israelian Beniamin Netaniahu[3], care a afirmat următoarele „*În urmă cu doi ani (2012) am stabilit un set de obiective pentru Israel pentru a deveni una dintre cele cinci mari puteri ale lumii în sectorul securității cibernetice. Acesta este un scop pe care l-am atins. Azi, Israel primește a cincea parte din investiția privată la nivel global din domeniul securității cibernetice.*[4]". Referințe directe despre această unitate apar în diverse surse deschise de informații, precum articolul privind tendințele și metodele acestei unități de a recruta posibili candidați care să activeze în sectorul cibernetic[5].

1. Gary Brown, Christopher D. Yung, „Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity", 19 ianuarie 2017 https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/, accesat în data de 29.11.2018.
2. CyberTech, The event for cyber industry, https://www.cybertechisrael.com/cybertech-tlv-2017, accesat în data de 29.11.2018.
3. Cabinetul Primului Ministru Israelian, „PM Netanyahu's Remarks at the Cyber-Tech Conference", 26.06.2017; http://www.pmo.gov.il/English/MediaCenter/Speeches/Pages/speechCyber260617.aspx, accesat în data de 29.11.2018.
4. „How Israel Rules The World Of Cyber Security | VICE on HBO" https://www.youtube.com/watch?v=ca-C3voZwpM, accesat în data de 29.11.2018.
5. Jared Coseglia, LegatTech News, „Unit 8200 CEO takes accelerated learning to the cyber masses", 16 ianuarie 2018, https://trustaffingpartners.com/uploaded/articles/

Dinamica tradițională a puterii este, de asemenea, subminată de teorii de securitate cibernetică care reliefează faptul că țările, care au resimțit un progres tehnologic masiv și au adoptat soluții de guvernare și administrare digitale în detrimentul utilizării vechilor metode fizice, sunt fără de tăgadă și cele mai dependente de infrastructura digitală, devenind astfel și cele mai vulnerabile la un atac cibernetic major. Pe de altă parte, Lindsay Jon R., într-una din lucrările sale[1], susține că doar superputerile tehnologice posedă capacitatea de a dezvolta cele mai sofisticate arme cibernetice, ceea ce sugerează că domeniul asimetric al domeniului cibernetic poate fi supraevaluat.

Teoriile Școlii de gândire realiste evidențiază nevoia statelor de cunoaștere și înțelegere a impactului produs de capacitarea cibernetică a unui stat în raport poziționarea acestuia în termeni de putere cu celelalte state. În acest context, având în vedere și cele enunțate de Schelling Thomas C. în cartea *„Arms and Influence. New Haven"*, scrisă în 1966, putem observa și o altă perspectivă a realismului: o abilitate a unui stat de a induce dorința și nevoia unui alt stat de a provoca sau amenința un al de-al treilea stat (posibil inamic sau cu care se regăsește într-o formă de conflict), indiferent de repercusiunile și pagubele produse în urma acestei acțiuni. Chiar și în contextul mai sus menționat, există îndoieli majore cu privire la eficacitatea constrângerii în sectorul cibernetic, deoarece tehnologia nu are capacitatea distructivă a operațiunilor militare convenționale din clasicele teatre de operațiuni. Mai mult decât atât, aceasta este mai puțin probabil să fie luată în considerare de statul țintă ca o metodă militară[2]. De foarte multe ori, identificăm observatii în literatura cibernetică asupra

Unit%208200.pdf, accesat în data de 29.11.2018.

1. Lindsay Jon R., „Stuxnet and the Limits of Cyber Warfare", în *Security Studies*, Vol. 22, Nr. 3, Taylor&Fracis Online pp.365–404, https://www.researchgate.net/publication/271930065_Stuxnet_and_the_Limits_of_Cyber_Warfare, accesat în data de 29.11.2018.
2. Gartzke Erik, „The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", în *International Security*, Vol.38, Nr. 2, pp.41–73, http://pages.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf, accesat în data de 29.11.2018.

limitelor războiului online, bazat pe resursele internetului, prin definiții precum „*Capabilitatea de paralizie din partea unui atacator asupra infrastructurii, sistemului de comunicații sau capacităților militare ale unui stat este una și cu totul alta este atunci când acesta se asigură că daunele provocate în urma acestei „paralizii" de sistem se transpun într-o schimbare considerabilă la nivelul echilibrului unui stat în a rezolva acest lucru.*[1]" Consider și sugerez că armele cibernetice pot fi eficiente doar atunci când sunt utilizate simultan cu operațiunile militare convenționale. Această afirmație este puternic argumentată de un studiu statistic privind eficacitatea diferitelor metode ofensive în plan cibernetic. Valeriano și Maness[2] analizează datele despre incidente cibernetice între statele rivale și constată că acțiunile cibernetice coercitive care vizează schimbarea comportamentală a țintei sunt, în general, ineficiente dacă le comparăm cu perturbările la scară mică sau spionajul.

Aceste constatări sugerează că noțiunile tradiționale de „*putere*" și de „*război*" nu sunt neapărat traduse sau transpuse în domeniului cibernetic. Totodată observăm că puterea din sectorul cibernetic nu este o putere care să poată revoluționa conceptul și demersul politicii internaționale.

III.1.5. Neorealismul și distribuția puterii

Ca multe alte teorii, realismul a evoluat de-a lungul timpului. Neorealismul, denumit și realism structural, se concentrează mai degrabă pe structura și distribuția puterii în sistemul internațional decât pe caracteristicile de putere ale statelor percepute individual. Un concept cheie în neorealism este cel al polarității, care descrie structura de putere din sistemul internațional. Astfel, un pol poate fi perceput ca un stat care este un centru de putere, care îi atrage pe alții în sfera

1. Gartzke Erik, *op. cit.* p.2.
2. Valeriano Brandon, Ryan C. Maness., *op.cit* pp.164-187, https://www.researchgate.net/publication/282792147_Cyber_War_versus_Cyber_Realities_Cyber_Conflict_in_the_International_System, accesat în data de 03.12.2018.

sa de influență, asemenea polului unui magnet, care atrage pilitura metalică sau așa cum gravitatea soarelui atrage planetele pe o orbită în jurul său.

În ceea ce privește interesul statelor de a identifica un model de participație ideal pentru toate statele în armonia unui sistem internațional unic, una dintre dezbaterile majore a fost cea privitoare la posibilitatea reconfigurării polilor de putere în lumina teoriei echilibrului de putere[1] - multipolară, bipolară sau unipolară - pentru a găsi echilibrul și a gestiona această nouă formă comun agreată în crearea unei lumi mai pașnice.[2]

Specialiștii din domenii diferite prognozează un final al configurației unipolare a ordinii mondiale şi începutul uneia multipolare. Se pot aduce în prim plan două dintre premisele acestei tranziții. Prima rezidă în natura riscurilor şi amenințărilor contemporane la adresa securității. În prezent se pornește de la premisa că nici un actor al arenei internaționale nu este autosuficient în a-și asigura unilateral securitatea. Strategiile externe și conceptele de securitate [3],[4],[5], strategiile de securitate națională ale statelor membre UE și NATO sau a altor state partenere întăresc ideea că cea mai eficientă abordare în obținerea unui grad optim de securitate în context internațional este reconceptualizarea și reformarea securității naționale, securității regionale şi internaționale în termenii comuni statelor partenere.

1. Teoria echilibrului de putere susținută de Hans J. Morgenthau, Henry Kissinger, Martin Wight.
2. Milja Kurki, Steve Smith, *Internationale Relations Theories. Discipline and Diversity*, Ed. Oxford University Press, Oxford, 2006, pp.71–88.
3. Office of the Director of National Intelligence, SUA, „2019 National Intelligence Strategy" https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy, accesat în data de 28.08.2020.
4. Comisia Europeană, Shared Vision, „Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy", http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accesat în data de 28.08.2020.
5. NATO, Noul Concept Strategic al NATO: O perspectivă parlamentară, https://www.nato.int/docu/review/2009/0902/090203/RO/index.htm, accesat în data de 28.08.2020.

O a doua premisă a tranziției de la unipolarism la multipolarism este de sorginte pur economică[1], unde nu se discută în termenii realismului clasic despre posibilitatea emergenței unui conflict sau crearea de coaliții ori alianțe pentru menținerea echilibrului de putere. Tendința generală este de abordare a unor strategii și parteneriate în vederea cooperării pentru atingerea unor interese și obiective comune.[2] Distribuția unor astfel de capacități între state este considerată ca având implicații semnificative pentru stabilitatea sistemului internațional, mai ales din perspectiva securității naționale.

Să aruncăm o privire rapidă asupra modului în care sistemul internațional poate fi structurat în viziunea realismul structural. Sistemele multipolare sunt cele care dețin sau au în componență mai multe centre de putere diferite și fiecare stat din sistem acționează relativ-independent unul de celălalt. Europa secolului al XIX-lea este un exemplu concret și destul de evident. Se poate aduce în acest context un exemplu din istoria UE, unde în secolul XIX-XX, supranaționalitatea în calitate de principiu de drept stă *„la baza unor organisme și organizații internaționale (vezi Tribunalele Internaționale, Organizația internațională a Muncii, Curtea Permanentă de Justiție Internațională), dar a primit o accepțiune concretă numai în Tratatul instituind Comunitatea Cărbunelui și Oțelului (Paris 18 aprilie 1951)"*[3].

Un sistem bipolar este unul în care există două state care servesc ca centre de putere relativ egală. Alte state din sistem gravitează în jurul unuia dintre cele două centre de putere din alianță și sunt dominate de acesta. Războiul rece dintre Uniunea Sovietică și Statele Unite ale Americii este un exemplu al unui sistem bipolar în care

1. Exemplul strategiilor economice ale statelor BRIC (*Brazilia, Rusia, India, China*) în perioadele de criză în perioada 2000-2020.
2. Cristina Bogzeanu, „Echilibrul de putere şi mediul de securitate", în *Implicații ale teoriilor echilibrului de putere şi a echilibrului de interese într-un sistem internațional multipolar (conference proceedings)*, Edit. Universității Naționale de Apărare „Carol I", Bucureștii, 2011, pp.65-67.
3. Ivan Adrian-Liviu, *Statele Unite ale Europei: Uniunea Europeană între interguvernamentalism şi supranaţionalism*, Editura Institutul European Iaşi, Iași, 2007, p.45.

lumea a fost împărțită între cei „aliați” cu U.R.S.S. și cei „aliați” cu Statele Unite ale Americii.

Un sistem unipolar, numit și sistem hegemonic, există atunci când un stat, numit un hegemon, este capabil să domine sistemul internațional, permițându-i să determine regulile prin care relațiile politice și economice sunt realizate de și între state. Unii susțin că, după Războiul Rece, am intrat într-o lume unipolară în care Statele Unite joacă rolul de hegemon.

În ultimele două decenii, am asistat la o schimbare de paradigmă a distribuției puterii la nivel global, aceasta transferându-se într-un procent inexact și foarte dinamic către Statele Unite ale Americii, China și Rusia. John Joseph Mearsheimer[1], într-un interviu orientat pe manifestările realismului în sectorul politic, oferă ca exemplu un studiu comparativ între Statele Unite ale Americii și România. Acesta afirmă că SUA este o țară extrem de puternică și în plus aceasta nu are vecini în emisfera vestică care ar putea să prezinte vreo amenințare militară în vreun fel. În ceea ce privește România, aceasta întotdeauna a fost o țară relativ mică, care a fost mereu înconjurată de țări foarte puternice, precum Germania, Imperiul Austro-Ungar, Imperiul Otoman, Uniunea Sovietică sau Rusia. Iar când ești mic și înconjurat de țări mari, trebuie să fii foarte deștept ca să supraviețuiești. Pentru a sparge mitul amenințării directe și iminente din partea Federației Ruse asupra României, acesta vine cu două motive, anume, precizează că Rusia nu mai este atât de puternică, fapt resimțit din plin în ultimii ani și pe măsură ce timpul trece puterea Rusiei va intra în declin. Federația Rusă nu va crește în putere în viitorul apropiat. Locul sau poziția Rusiei începe sa fie ocupat din ce în ce mai vizibil de Republica Chineză[2].

1. Portal: http://mearsheimer.uchicago.edu/, accesat în data de 16.10.2018.
2. Interviu John Joseph Mearsheimer, TVR 1, 14.11.2018.

III.1.6. Punctele tari și puncte slabe ale realismului

La fel ca majoritatea teoriilor politice, realismul are atât puncte forte cât și puncte slabe. Neorealismul se concentrează pe unele dintre cele mai importante aspecte ale relațiilor internaționale, precum războiul, prevenirea războiului, echilibrul puterilor, alianțele și cursele de înarmare. Totodată, cunoașterea acestor interese este un bun început în înțelegerea problemelor existente în istoria și relația statelor din sistemul internațional. Se pot aduce contribuții importante în înțelegerea conflictelor și prevenirea acestora chiar înainte de a începe, oferind o înțelegere a puterii și a modului de acțiune a statelor.

Deși realismul poate uneori explica foarte multe despre scena relațiilor internaționale, rareori dă imaginea de ansamblu, acesta fiind concentrat pe o analiză introspectă a situațiilor în care statele sunt implicate. Majoritatea consideră că susținătorii realismului subliniază puterea militară și economică ca monedele puterii și ignoră contribuțiile culturii și ideologiei ori identității naționale. În timp ce statele sunt încă actorii dominanți pe scena mondială, rolul organizațiilor guvernamentale internaționale, precum ONU și Banca Mondială, al organizațiilor nonguvernamentale, precum Crucea Roșie și al marilor corporații internaționale, devine din ce în ce mai seminificativ.

Mai mult, statele nu acționează întotdeauna doar pentru exercitarea puterii, așa cum demonstrează cooperarea internațională în eforturile de ajutor umanitar în timpul dezastrelor sau cataclismelor. În cele din urmă, viziunea teoriei asupra lipsei de importanță a eticii în relațiile internaționale nu reușește să găsească sprijin în mișcarea globală tot mai mare îndreptată înspre drepturile omului recunoscute pe plan internațional. Pe scurt, realismul oferă un model prea simplu pentru a explica în totalitate situația complexă a relațiilor internaționale.

III.1.7. Realismul aplicat: securitatea cibernetică

Unul dintre rezultatele obținute în urma primei analize asupra Războiului Peloponez (secolul V î.Hr.) a fost identificarea naturii amorale

a acțiunilor politice în context internațional și relevanța factorului de putere obținut și manifestat de state în vederea obținerii unei recunoașteri sau supremații politice în relația cu statele aliate sau în raport cu inamicii (statali și non statali). O evoluție realistă a teoriei relațiilor internaționale poate fi atribuită lui Hans Morgenthau, care a avut în vedere înțelegerea, teoretizarea și tratarea echilibrului de putere între statele care acționează rațional și se auto-interesează.

Realismul, ca școală de gândire și aplicarea teoriilor ce o susțin, reprezintă încă o paradigmă dominantă în sistemul relațiilor internaționale. Realismul este bine definit în acest context, dar nu își poate asuma rezolvarea definitivă a dilemei de securitate cibernetică. Arealul cibernetic aduce noi perspective și oportunități influențate de realism, orientat în mod deosebit pe securitate și competiție, pe redistribuirea puterii în plan regional și global, pe avantajul viziunii ofensive asupra viziunii defensive și *„beneficiile strategiilor de descurajare, oferind astfel o oportunitate de a evalua rolul realismului în aceste dezbateri nerostite"*[1].

Teoria realismului, având în general ca preocupare problematica securității și factorul de putere națională, pare a fi una dintre perspectivele și instrumentele preferate în procesul de analiză a conflictelor din sectorul cibernetic în contextul relațiilor internaționale. Realismul rămâne un cadru relevant pentru identificarea problemelor importante legate de securitate în domeniul cibernetic și poate oferi uneori informații utile în ceea ce privește unele caracteristici ale relațiilor internaționale. Cu toate acestea, teoriile realiste despre conflicte adesea nu sunt suficient de relevante în ceea ce privește explicarea dinamicii unice a conflictului cibernetic sau în crearea unei prognoze obiective asupra conflictelor.

Având în vedere statutul lacunar al teoriilor realismului în context de securitate cibernetică, atât practicienii din sectorul de securitate, cât și cercetătorii încurajează dezvoltarea de noi teorii bazate pe

1. Anthony J.S. Craig, Brandon Valeriano, *Realism and Cyber Conflict: Security in the Digital Age*,Edit. E-International Relations Publishing, Bristol, Anglia, 2018, p.86.

observație empirică sau logică deductivă a domeniului cibernetic. Prin dezvoltarea cercetărilor empirice, putem înțelege mai exact problematica impactului provocat de cursele de înarmare cibernetică în raport cu relațiile interstatale, distribuirea capacităților cibernetice între actorii statali și nestatali, precum și motivele reținerii acestora în cazul unei oportunități ofensive. Obținerea unor răspunsuri concrete, clare și obiective la aceste întrebări ne poate ajuta la formularea unei orientări politice mai bune pentru guverne sau chiar a unei reconceptualizări a dimensiunii politice naționale și internaționale.[1]

Doresc să ofer o privire de ansamblu asupra teoriei realiste și a modului în care aceasta se referă la securitatea cibernetică înainte de a aborda un set de subiecte specifice, influențate de realism, în cadrul discursului actual de securitate cibernetică.

Analizând rezultatele, am ajuns la concluzia că relevanța realismului este reprezentată de faptul că ne oferă o teorie descriptivă și prescriptivă a comportamentului de stat în domeniul cibernetic. În sectorul relațiilor internaționale contemporane, se susține faptul că, deși realismul poate contribui la ridicarea chestiunilor cheie în securitatea cibernetică, perspectiva generală nu are capacitatea de a explica dinamica conflictului cibernetic.

În ceea ce privește neorealismul, care a apărut în jurul anilor 1970, odată cu apariția acestuia s-a evidențiat și o diviziune între realismul defensiv și realismul ofensiv. Ambele filosofii au puncte comune, precum acordul asupra faptului că supraviețuirea este motivul primar al statului, dar trebuie subliniat faptul că pentru realiștii defensivi, majoritatea statelor sunt puteri ale căror *status quo* urmăresc un echilibru de putere, menținând astfel un sistem internațional operațional și stabil. Pe de altă parte, realiștii ofensivi, susțin că statele urmăresc să obțină pe cât posibil toată puterea, având ca obiectiv primar asigurarea supraviețuirii acestora într-un sistem predominant anarhic. Cea mai recentă componentă a realismului este realismul neoclasic,

1. *Ibidem*, pp.94-95.

care explică comportamentul statului nu doar pe factori structurali, ci și variabilele de nivel național, inclusiv percepțiile greșite ale factorilor de decizie.

Realismul a fost supus unei mari presiuni, constante și reale, provenite din lipsa capacității de a explica comportamentul statului sub doctrina realismului sau de a oferi orientări eficiente în materie de politici. Studiile și cercetările în domeniul relațiilor internaționale indică adesea lipsa dovezilor conform cărora statele acționează în conformitate cu logica echilibrului puterii, o ipoteză proeminentă în literatura realistă. Predicțiile generate, contradictorii de altfel, precum și lipsa progresului empiric îi determină pe diverși experți contemporani, precum John A Vasquez[1], să cpnsidere realismul ca fiind o paradigmă „degenerativă" mai degrabă decât „progresivă". Mai mult, studiile statistice sugerează că factorii considerați de realiști a spori securitatea națională, cum ar fi construirea și alianțele militare, nu se remarcă aproape defel printr-o productivitate a statelor (în deosebi a celor *„vasal"*), ci sporesc probabilitatea unui conflict între acestea[2]. Cu toate acestea, cu accentul pus pe problemele de securitate și de conflict, realismul pare a fi teoria naturală pentru a elucida problemele de securitate cibernetică.

Se presupune că primele studii privind conflictele cibernetice au început atunci când Arquilla și Ronfeldt[3] au introdus conceptele de „cyberwar" (trad. eng. *război cibernetic*) și „netwar" (trad. eng. *război în rețea*) și au prezis o transformare a războiului în concordanță cu progresele rapide ale tehnologiei informației și a comunicației. Această formă de conflict are loc în general în spațiul cibernetic, un mediu

1. John Vasquez, „The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition", în *The American Political Science Review*, Vol. 91, Nr. 4, 1997, pp.899–912.
2. Senese Paul D., John A. Vasquez, *„The Steps to War: An Empirical Study"*, Ed.Princeton University Press, Princeton, SUA, 2008.
3. John Arquilla, David Ronfeldt., „Cyberwar is Coming!", în *Comparative Strategy*, Vol.12, Nr. 2, 1993, pp.141–165.

definit simplu ca *„toate rețelele de calculatoare din lume și tot ceea ce se conectează și controlează”*[1]. Conflictul cibernetic se rezumă în deosebi la *„utilizarea tehnologiilor computaționale în spațiul cibernetic în scopuri malițioase și / sau distructive, pentru a influența sau modifica interacțiunile diplomatice și militare dintre entități”*[2]. În ceea ce privește impactul asupra securității naționale, consider că trebuie să ne concentrăm atenția în mod deosebit pe aceste tipuri de „intervenții”, care sunt efectuate din punct de vedere criminologic la un nivel net superior, cu rezultate de anvergură, fără de tăgadă acestea fiind motivate politic.

Printre interesele primare ale statelor în ceea ce privește securitatea națională, în contextul geopolitic actual, sunt amenințările din sectorul cibernetic, avertismentele din acest sector sunt predominant împotriva atacurilor cibernetice asupra infrastructurilor critice vulnerabile. În 2012, de exemplu, Secretarul American al Apărării a avertizat asupra unui posibil „Pearl Harbor” cibernetic care poate să aibă în obiectiv rețelele de furnizare a energiei electrice sau sistemul financiar național, ambele fiind operaționale la acea dată prin intermediul rețelelor informatice și de comunicații [3].

Potrivit unui sondaj din 2016, 73% dintre americani au crezut că terorismul cibernetic reprezintă o *„amenințare critică”* pentru sistemul de securitate al Statele Unite ale Americii.[4] Conform comentariilor unor analiștilor de profil, se aduce în linia întâi această amenințare numind-o *„amenințare foarte reală și presantă pentru securitatea națională”*, însă cei mai mulți cercetători devin vocali expunând rezultate prin care nivelul de risc nu este conform titlului oferit de cei doi,

1. Richard A.Clarke, , Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* New York: Ecco. SUA, 2010, p.70.
2. Valeriano Brandon, Ryan C. Maness., *op.cit.*, p.32.
3. Elisabeth Bumiller, Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.”, Jurnalul *The New York Times* din 11.10,2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html, accesat în data de 21.11.2018.
4. McCarthy Justin, “Americans Cite Cyberterrorism Among Top Three Threats to U.S.”, 10.02.2016, https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx, accesat în data de 21.11.2018.

aducând argumente cum că această amenințare este exagerată[1]. În aceeași ordine de idei, în literatura internațională de specialitate, fenomenul „cyberwar" (*războiului cibernetic*) nu este reprezentat la magnitudinea unui război tradițional, iar probabilitatea declanșării unui astfel de război în viitor este puțin probabilă. De asemenea, empiric este demonstrat atât nivelul slab al incidenței unui război cibernetic, cât și gravitatea scăzută a unui posibil conflict cibernetic față de dimensiunea unui război între state rivale. Pentru a demonstra percepția ridicată în ceea ce privește iminența unui război cibernetic, unii experți adoptă teoria securitizării[2] [3].

În ceea ce privește aplicarea teoriilor realismului, studiul securității cibernetice este orientat și spre analiza celor mai importante surse generatoare de insecuritate, anume asupra oportunităților și mecanismelor utilizate de grupările teroriste în mediul virtual sau în mediul real cu efecte în mediul cibernetic.

Putem afirma că studiul terorismului contemporan abordează în mod special problema terorismului din trei perspective[4]:

A. Măsura în care noile tehnologii, precum internetul în ansamblul său și echipamentele de comunicații moderne, influențează și facilitează crearea de noi metode de organizare teroristă aplicată la contextul social contemporan;
B. Rolul convingerilor religioase ca principii de organizare, care întăresc coeziunea rețelelor teroriste, oferindu-le astfel un grad ridicat de letalitate;

1. Rid Thomas, *Cyber War Will Not Take Place*, Edit. C Hurst & Co Publishers Ltd., Londra ,2013.
2. Clara Eroukhmanoff, „Securitisation Theory: An Introduction", E-International Relations Students, 14.01.2018, https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/, accesat în data de 21.11.2018.
3. Cavelty Myriam Dunn, „Cyber-Security and Threat Politics: US efforts to secure the information age", în *CSS Studies in Security and International Relations*, Prima Ediție, Edit. Routledge, London, UK, 2008.
4. David Wright-Neville, *Dicționar de Terorism* (traducere Sorina Pricop), Edit. CA Publishing, Cluj-Napoca, 2010, p.231.

C. Lipsa nevoii unui lider și capacitatea celulelor teroriste de autogenerare.

Rezumându-mă strict la prima perspectivă, pot afirma, bazat pe experiențele ultimilor ani (2015-2018) că noul terorism utilizează unul dintre elementele care formează sau deformează păreri, opinii și convingeri, anume componentele media și publicitatea. Pentru a-și atinge scopul, noul terorism, prin caracterul său amorf și utilizând resursele evoluției tehnologice și informaționale, produce noi metode și tehnici de intimidare, descurajare, pedepsire, umilire, sau distrugere a celor care se opun cursului propus de indivizii, celulele sau organizațiile teroriste. În altă ordine de idei, actele teroriste, indiferent de magnitudinea lor, pot fi percepute strategic, ca joc politic, unde actele de violență - în mediul fizic sau virtual - și carnagiul produs sunt doar un scenariu atent regizat cu un singur scop, cel de a transmite un mesaj. Pentru ca această strategie să își atingă scopul este imperios necesar să existe o audiență sau un public care să fie sensibilizat.

Din perspectiva media, ca mediu de difuzare a prezenței și acțiunilor teroriste, promotorii violenței teroriste utilizează mijloacele media - ex. *casa de producție al-Qaeda: as-Sahab* - pentru a comunica cu două tipuri distincte de public:

- „out-grupul" (*grup ușor de intimidat și terifiat*);
- „in-grupul" (*grup ușor de inspirat, manipulat și convertit*)[1].

Având în vedere cele mai sus menționate, deducem într-un mod natural existența unei legături între terorismul obișnuit și noul terorism, unde formațiunile teroriste din lumea întreagă au început să își dezvolte arsenalul de propagandă și inducere a terorii. Așadar, există o tendinta generala de a minimiza acest fenomen, argumentând că un atac cibernetic nu poate fi considerat un atac precum cel din Estonia din 2007, unde ținta a fost întreaga structură informațională (privată, publică, guvernamentală șamd.) a țării. După cum bine

1. *Ibidem*, p.219.

cunoaștem, atacuri precum cele cu o arie mai mare de răspândire, precum WanaCry, sau atacuri orientate spre infrastructura critică cu implicații de securitate națională pot ușor fi percepute ca acte de terorism. Acest punct de vedere este actualmente larg răspândit, iar formularea mai amplă a definiției terorismului îl identifică pe acesta ca fiind reprezentat de *„uzul de tehnologie de către grupări teroriste recunoscute pentru sabotarea sistemelor informatice critice (cum ar fi cele care controlează traficul aerian, comunicațiile sau sistemele de aprovizionare cu energie) cu scopul de a cauza daune masive sau pentru a crea panică. Într-o altă ordine de idei, putem afirma că terorismul cibernetic reprezintă utilizarea premeditată și motivată politic a tehnologiilor informaționale cu scopul de a crea panică, daune sau chiar moartea"*[1].

După cum aminteam mai sus, realismul este considerat un cadru filosofic util, cu ajutorul căruia putem înțelege anumite perspective ale spațiului cibernetic. Dintr-o altă perspectivă conceptuală, se poate genera afirmația că *„teoriile realiste ale descurajării, gestionării crizelor și ale conflictului pot fi folosite pentru a înțelege dacă spațiul cibernetic este stabilizator sau destabilizator, dacă tehnologiile cibernetice vor reprezenta o nouă sursă de conflict sau de pace și dacă statele se vor angaja în curse de armare cibernetică"*[2].

III.1.8. Conceptul de anarhie în contextul securității cibernetice

Anarhia este definită ca „1. *Dezordine produsă într-un stat prin lipsa de guvernământ sau prin slăbiciunea celor care guvernează. 2. Lipsă a unei puteri, a unei conduceri. 3. Dezorganizare. 4. Lipsă de supunere față de legi sau de autorități*[3]". Totodată, aceasta este presupunerea fundamentală

1. Ibidem, 136.
2. Reardon Robert, Nazli Choucri, *"The Role of Cyberspace in International Relations: A View of the Literature"*. Lucrare prezentată în 2012 la Convenția Anuală ISA, San Diego, California, SUA, 01.04.2012, p.7, https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf, accesat în data de 21.11.2018.
3. Academia Română, Institutul de lingvistică *„Iorgu Iordan"*, *Mic dicționar academic*, Ediția a II-a, Edit. Univers Enciclopedic , București, 2010.

care stă la baza teoriilor structurale realiste și se referă la lipsa unei autorități globale care să arbitreze „*sistemul internațional*" care insuflă un sentiment de neîncredere între state[1]. De aici vine și resimțita obligativitate a statelor de a iniția și susține măsuri de autoapărare în tot ceea ce aparține sectorului securității naționale și de a-și continua demersurile în vederea atingerii intereselor sale naționale. Cât despre poziția realiștilor defensivi, aceștia consideră că o mare parte din cauzele conflictelor provin din competiția dintre statele, care devin pro-active în contextul asigurării securității în ambele dimensiuni, național și individual. Dilema de securitate descrie și fenomenul prin care „multe dintre mijloacele prin care un stat încearcă să-și sporească securitatea scad în egală măsură securitatea celorlalte state[2]".

Acțiunile, cum ar fi întărirea și înzestrarea sectorului militar cu mijloace moderne, sau încheierea de alianțe cu alte state, sunt adesea percepute de celelalte țări ca o reală amenințare, acestea adoptând ulterior măsuri similare sau superioare doar pentru a-și spori propria securitate. Acest proces este adesea numit modelul spirală, fiecare acțiune provocând o reacție[3]. De asemenea, este important de menționat faptul că măsurile luate de țările observator (în acest caz) sunt luate în raport cu nivelul de măsuri adoptate și cu tipul de interese atinse în cadrul alianțelor încheiate, precum și cu gradul de putere al statelor care se aliază[4]. Modelul spirală se află în centrul conceptualizărilor tradiționale ale unei curse a înarmărilor, despre care se spune că provoacă schimbări rapide în balanța puterii, o creștere a

1. Kenneth N. Waltz, *Theory of International Politics*, Edit. Addison-Wesley Publishing Company, Londra,1979, pp.102-128.
2. Jervis Robert, "Cooperation Under the Security Dilemma", în *World Politics*, Vol.30, Nr. 2,, Edit. The Johns Hopkins University Press, 1978, p. 169, http://www.jstor.org/stable/2009958, accesat în data de 09.12.2018.
3. Charles L. Glaser, „When Are Arms Races Dangerous? Rational versus Suboptimal Arming", în *International Security*, Vol.28, Nr. 4, 2004, p. 44, https://www.belfercenter.org/sites/default/files/files/publication/glaser.pdf, accesat în data de 04.12.2018.
4. Ipotetic, reacția SUA la o alianță între România și Turkmenistan în ceea ce privește sectorul energetic nu ar fi atât de evidentă față de o alianță similară, dar între România și Rusia sau China.

tensiunilor internaționale și un risc crescut în raport cu posibilitatea de conflict[1].

Paradigma realistă are o viziune clară asupra conceptului de anarhie și în ceea ce privește efectele acesteia înțelegem în mare parte cum spațiul cibernetic funcționează. Aceste aspecte pot fi puse cu ușurință sub lupa analiștilor, chiar și a celor mai puțin experimentați, care vor identifica că acest areal virtual pare a fi condus într-o proporție covârșitoare de aceste principii ale anarhiei. Teoreticienii studiilor relațiilor internaționale liberale susțin că efectele periculoase ale anarhiei pot fi ameliorate de instituțiile promotoare în procesul de globalizare, care au capacitatea de a media disputele interstatale și care pot echilibra prin eliminarea incertitudinilor, aducând informația necesară[2]. Când facem referire la domeniul cibernetic ori arealul cibernetic din perspectivă limitativă, „geografică", observăm că acesta nu are parte de o guvernare instituțională la nivel global. Formele de guvernare ale spațiului virtual sunt cele primare, reprezentate generic de organismele care reglementează domeniile www sau diverși furnizori de servicii de internet, iar dintr-o perspectivă guvernamentală avem ministerele de resort IT&C, care încearcă prin metode realiste să reglementeze accesul în spațiul virtual pe teritoriul geografic al statelor ori a persoanelor ori serviciilor IT&C din exteriorul statului. Printre organizațiile relevante la nivel global se numă Uniunea Internațională pentru Telecomunicațiilor (ITU)[3] și Corporația Internet pentru Nume și Numere Alocate (ICANN)[4], însă atribuțiile, competențele și influențele acestora nu se extind la nivel de gestionare a conflictelor la nivel global.

1. John A. Vasquez, *The War Puzzle*, Cambridge University Press, Cambridge, 1993, pp. 167-213.
2. Russett Bruce, John Oneal, *Triangulating Peace, Democracy, Interdependence, and International Organizations*, Edit. W.W. Norton & Company, New York-Londra, 2001, pp.157-193.
3. https://www.itu.int/en/Pages/default.aspx, accesat în data de 27.11.2018.
4. https://www.icann.org/, accesat în data de 27.11.2018.

III.1.9. Cursa înarmărilor cibernetice

În ceea ce privește rapoartele apărute în media cu privire la o posibilă cursă a înarmărilor cibernetice, acestea sunt din ce în ce mai frecvente[1 2 3], iar această tendință a militarizării statelor în spațiului cibernetic este evidentă. Semnale clare ale înarmării sunt și apariția unor noi organizații militare sau forme de organizare militară la nivelul armatelor statelor, elaborarea unor doctrine și strategii cibernetice în sectorul militar, creșterea bugetelor pe sectorul dezvoltării și inovării securității cibernetice, precum și angajarea „războinicilor" cibernetici. Putem să ne creăm o viziune de ansamblu privind zona de dezvoltare în sectorul cibernetic doar privind asupra programelor malițioase precum „Stuxnet", care a fost dezvoltat în cel mai mare secret și utilizat exact în ideea atingerii scopurilor realiste ale unei țări privitoare la un alt stat care era generator de insecuritate la nivel global. Putem afirma că în arsenalul militar al unei țări poate intra fără nici o restricție acest nou tip de „produs", deși intangibil extrem de periculos, arma cibernetică. În plus, un număr semnificativ de specialiști, jurnaliști, observatori sau rapoarte de securitate ale statelor oferă dovezi empirice care demonstrează o relație de interdependență între dezvoltarea sectorului cibernetic și percepțiile celorlalte state privind posibila amenințare cibernetică, precum și generarea unui spirit concurențial între state[4].

1. Steve Ranger, „Inside the secret digital arms race: Facing the threat of a global cyberwar", 12.09.2018, https://www.techrepublic.com/article/inside-the-secret-digital-arms-race/, accesat în data de 04.12.2018.
2. Vesa Kanniainen, „Cyber Technology and the Arms Race", în *HECER Discussion Paper No. 424*, Helsinki, 2018, pp.1-2, https://helda.helsinki.fi/bitstream/handle/10138/232974/HECER-DP424.pdf?sequence=1, accesat în data de 04.12.2018.
3. Gordon Corera, „Rapid escalation of the cyber-arms race", 29.04.2015, https://www.bbc.com/news/uk-32493516, accesat în data de 04.12.2018.
4. Anthony Craig, Brandon Valeriano, „Conceptualising cyber arms races", în *Proceedings of the 8th International Conference on Cyber Conflict (CyCon)*, Edit. NATO CCD COE Publication, Tallin, 2016, https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arms_races, accesat în data de 06.12.2018.

Cu toate că pare deja un clișeu, consider important să înțelegem faptul că realismul poate aduce lămuriri clare privind explicarea comportamentului statelor în ceea ce privește și cursa înarmării cibernetice ca pe un răspuns la acest nou tip de amenințare într-o lume anarhică[1]. De asemenea, constatăm că în ceea ce privește dilema de securitate cibernetică, aceasta este cu atât mai evidentă și greu de gestionat cu cât diferențele dintre capabilitățile defensive și cele ofensive, nu se disting. Severitatea în ceea ce privește tratarea dilemei de securitate cibernetică apare fără îndoială atunci când capacitățile ofensive și defensive în sectorul înarmării cibernetice sunt indiscutabile și evidente cu scopuri clare. În acest context, statele nu pot să transmită alte semnale sau să manifeste alte intenții decât cele privitoare la o posibilă amenințare din partea statelor dezvoltatoare de soluții în acest sector. În spațiul cibernetic, capacitățile cibernetice sunt foarte greu de identificat sau de distins. Este aproape imposibil de identificat un proces ofensiv precum atacul de tipul „*ziua 0*”[2], mai ales dacă acesta provine dintr-un sector guvernamental, deoarece acest tip de atac, precum și metoda de exploatare a acestuia, prin definiție sunt necunoscute. Putem exemplifica dificultatea identificării unui atac printr-o analiză succintă a specificului organizațiilor militare de profil în sectorul cibernetic, precum U.S. Cyber Comand[3], care tind să aibă atât roluri defensive, cât și roluri ofensive și care au posibilitatea de a-și mări bugetele sau redimensiona personalul la nivelul capacităților necesare. Cu toate că nu se regăsesc informații privind planurile de investiții ale acestor organizații, se poate înțelege din viziunea acestor entități că au misiunea de a direcționa, sincroniza și coordona planificarea și operațiunile cibernetice pentru a apăra

1. Jervis Robert, *op.cit*, pp. 186-194.
2. Bitdefender, „Detectați Atacurile de tip Exploit și Zero-Day”, https://www.bitdefender.ro/business/usecases/exploits-zero-days.html, accesat în data de 27.11.2018.
3. Vision Document as of April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, accesat în data de 27.11.2018.

și promova interesele naționale în colaborare cu partenerii interni și internaționali. Aceste aspecte sumare sporesc incertitudinea și concurența între state, făcându-le să își dorească totodată un nivel al securității net superior în spațiul cibernetic. Alianțele dintre state au rol decisiv în acest context deoarece, din dorința de a controla printr-o securitate „absolută", se fac concesii neorealiste cu o motivație realistă; apare o sincopă în funcționarea doctrinară a oricărui stat.

Pentru cei mai mulți realiști, cursa înarmării cibernetice crește probabilitatea apariției unui război[1][2], dar în ceea ce îi privește pe neorealiști, dezvoltarea militară în orice formă, reprezintă un mijloc eficient și necesar în descurajarea unei puteri revizioniste[3]. Așadar, apar și iminentele întrebări și supoziții privitoare la posibila escaladare de la competiția statelor în securizarea spațiului cibernetic la probabilitatea unui conflict real.

Studiile și cercetările în domeniu au demonstrat o relație între cursa înarmărilor și reacțiile militare internaționale și război[4][5]. Același interes vădit apare și la ipoteza înarmării cibernetice a statelor[6], fie acestea și într-o uniune ori alianță internațională. Va aduce această

1. Jervis Robert, *op.cit.*, p. 188.
2. Van Evera Stephen, "Offense, Defense, and the Causes of War", în *International Security*, Vol.22, Nr. 4, Edit. Cornell University Press, New York, 1998, p.13, https://pdfs.semanticscholar.org/48ea/f54d94f0abb9961f9a8fc09ac0f8f64ab103.pdf, accesat în data de 09.12.2018.
3. Charles L. Glaser, *op.cit.*, p.44.
4. Sample G. Susan, „Arms Races and Dispute Escalation: Resolving the Debate", în *Journal of Peace Research*, Vol. 34, Nr. 1, Edit. Sage Publications, 1997, p.17, http://www.jstor.org/stable/424827, accesat în data de 09.12.2018.
5. Gibler M. Douglas, Rider J. Toby, Hutchison L. Marc, „Taking Arms Against a Sea of Troubles: Conventional Arms Races During Periods of Rivalry", în *Journal of Peace Research*, Vol. 42, Nr. 2, Edit. Sage Publications, Ltd., Londra, 2005, pp.134, 141-144.
6. Paul Scharre, „Killer Apps: The Real Dangers of an AI Arms Race", https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?utm_campaign=site_visitor.unpaid.engagement&utm_source=facebook&utm_medium=tr_social&utm_content=72332040&_hsenc=p2ANqtz--65C7cpVxdnBIfZ5_OY-itxxPkXskZDGq8mqNC0NlU0VeCbGZ2H-NzuqH8G1fgZVTXEOnbBUim9wMQMS795xlW7fNAoMHLhYnZfOWaN8SddXeczUng&_hsmi=72332042&fbclid=IwAR0IbYfieSRq03n9ZWrvmJhDgr-rkXRLM-1dyMOXPy2gkb5DKYp-WROiutdk, accesat în data de 04.05.2019.

cursă de înarmare cibernetică la același rezultat ca și cursa înarmării tradiționale a statelor?

Conflictul din spațiul cibernetic este predispus într-un mod unic, dat de escaladarea incertitudinilor legate de ceea ce constituie, finalmente, un act de război și de numărul tot mai mare de actori statali și nestatali, care caută capacitarea sau înarmarea cu elemente cibernetice de tip ofensiv[1].

III.1.10. Analiza „spiralei” de (in)securitate cibernetică în context contemporan

Acest termen a apărut în jurul anilor 1950, datorită inițial lui John Hertz (1950), care de fapt i-a dat și numele, iar mai târziu mulțumită susținătorului acestei idei, Herbert Butterfield (1951) și nu în ultimul rând lui Robert Jervis (1970), care a dezvoltat ideea dilemei de securitate, ridicând ștafeta și aducând-o prin aprofundarea studiului securității în sectorul relațiilor internaționale la forma bine-cunoscută astăzi de model al spiralei de securitate sau insecuritate.

La o privire de ansamblu, empiric chiar, se poate identifica cu ușurință faptul că frecvența cu care apar diversele tipuri de conflicte cibernetice este tot mai mare, această creștere se corelează mai degrabă cu tacticile și strategiile de sabotaj și spionaj decât cu formele distructive precum războiul cibernetic[2]. Mai mult, datele arată că disputa interstatală în sectorul cibernetic este foarte puțin probabil să se propage într-o formă tangibilă precum războiului „clasic”, ceea ce sugerează că escaladarea conflictelor din acest sector este purtată într-o tendință dominantă de constrângere a oponentului. În ceea

1. Lord M. Kristin, Sharp Travis, *America's Cyber Future, Security and Prosperity in the Information Age*, Edit. Center for a New American Security, Washington, DC, 2011, p.29., https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf, accesat în data de 09.12.2018;
2. Valeriano Brandon, Ryan C. Maness., *op.cit*, p.17.

ce privește predicțiile modelului spiralat realist, statele par să evite escaladarea disputelor spre conflict, iar apoi spre un război.

Chiar și așa, dilema de securitate în context geopolitic și raportată la conflictele contemporane la nivel global, se transpune din plan fizic în plan cibernetic într-o proporție de 1:1. Cu toate acestea, de la terminarea celui de-al II-lea Război Mondial până acum, am asistat în plan european și cu mici excepții, în plan global, la una dintre cele mai lungi perioade de pace. Pe timp de pace și prosperitate majoritatea statelor au îmbrățișat ideologii bazate pe teoriile realismului, au întocmit planuri de măsuri la nivel național, agende strategice (5, 10, 20, 60 ani) și au dezvoltat instrumen defensive pentru un eventual conflict sau război.

Pe măsură ce un stat dezvoltă un sistem defensiv competitiv se declanșează un fenomen din partea statelor aflate la graniță sau în vecinătatea mai îndepărtată, ca o reacție de autoconservare a statelor din jur, care sporește gradul de insecuritate în toate planurile - politic, economic, uman șamd. Cu toate că granițele fizice nu mai reprezintă de multă vreme o limită pentru asigurarea securității naționale, prin intrarea în acest joc al luptei pentru putere cibernetică, suntem nevoiți să venim azi cu o schimbare de optică și chiar de dilemă de securitate națională. Dacă până acum câțiva ani vorbeam cu emoție de anumite arme care ajungeau la sute de kilometri distanță de la lansare la destinația țintă într-un timp de ordinul orelor sau minutelor, acum vorbim de atacuri inopinate cu un efect similar dacă nu sporit într-un timp record - în timp real. Noutatea în arealul cibernetic este că nu se mai poate prognoza un atac, acesta fiind identificat în momentul în care a fost lansat. Momentul lansării unui atac reprezintă, datorită progresului tehnologic, și momentul impactului acestuia asupra țintei. Am ajuns să ne obișnuim cu atacuri de tipul „*zero day*", APT sau atacuri hibride inopinate direcționate înspre mai multe ținte simultan, cu impact din ce în ce mai mare asupra sistemelor informaționale naționale și internaționale.

În aceste momente se poartă discuții mai mult sau mai puțin diplomatice care au ca scop principal dezarmarea nucleară, provenită tocmai din motive obiective susținute de ideologia realistă a statelor, cu rezultate mai puțin favorabile în interes global și favorabile celor puțini. Întrebarea care natural apare este cu privire la existența sau modalitatea de dezarmare digitală a unei țări. Nu există un termen de comparație între puterea nucleară și cea digitală, dar impactul financiar, social și militar poate fi comparat. Cel mai adesea este nevoie de reamintirea faptului că dezarmarea poate fi făcută acolo unde există un mijloc de atac, pe când în domeniul cibernetic, armele sunt dezvoltate de diverși actori, fiind bazate pe alte principii decât cele convenționale din mediul real.

În acest context ipotetic al nevoii de dezarmare digitală a unui stat națiune, care sunt implicațiile și care este dimensiunea daunelor colaterale aduse nu doar sectorului guvernamental, ci și celui civil? Dacă dimensiunea adusă de dezarmarea nucleară a unei țări este de ordin militar și este destul de puțin probabil să se răsfrângă direct asupra sectorului civil sau asupra sectorului public-privat, în contextul unei incapacități sau dezarmări digitale, simptomele vor fi resimțite în raport invers în rândul populației.

Este prematur să afirmăm faptul că escaladarea situațiilor poate deveni o tendință în tratarea conflictelor din acest nou areal, dar experiența a peste treizeci de ani de conflict în sectorul digital demonstrează și întărește acest grad remarcabil de bună gestionare pașnică a statelor care au evitat modele, tehnici, tactici și strategii distructive, precum și violența în spațiul cibernetic.

Evenimentele din perioada 2015-2020 sunt de fapt o continuare a unei perioade marcate de escaladare a tensiunilor statale la nivel european și global. Exemple precum tensiunea generată de relații dificile și adesea conflictuale - NATO - Rusia, SUA - Rusia, SUA - Coreea de Nord - duc la paralizarea comunității internaționale și incapacitatea de a adopta o poziție unitară în vederea asigurării unui climat sigur

în zonele de conflict, precum este Siria. În același context, regăsim state care susțin conflictul în anumite zone pentru a servi drept punct de vedere geopolitic și de raportare la capacitatea militară a acestora, în scopul obținerii unui drept de veto în soluționarea problemelor regionale ori globale.[1]

Cu toate că dilema de securitate este un termen utilizat cu preponderență în situațiile ce impun o analizare a stării de securitate în timpul conflictelor, în ultimii ani această sintagmă și-a schimbat oarecum definiția. O altă perspectivă de a interpreta această dilemă este prin utilizarea modelului de spirală de securitate, în care elementele constitutive ale analizei nu sunt exclusiv interdependente unele de altele, ci aduc rezultate separate. O exemplificare a celor expuse mai sus este grafic exprimată în hărțile relaționale de mai jos. În ceea ce privește conflictele, observ o oarecare amprentă unică și o raportare a acestora din orice alt plan în plan cibernetic. Nu încape îndoială faptul că foarte multe din aceste atacuri sunt duse la îndeplinire de atacatori cibernetici care acționează „pe cont propriu" și nu sunt efectuate de state. Referind-mă strict la România, în data de 22 septembrie 2018, la ora 18:00, asupra acesteia au fost lansate atacuri de tip DDoS din țări precum Sri Lanka, Quatar, Panama, iar mai apoi, escaladând în dimensiune, atacurile cele mai puternice fiind din țări precum Coreea de Nord, China, Africa de Sud, Franța, Germania și multe altele. În majoritatea cazurilor, cu o mare ușurință se pot ușor identifica sursele de atac, tipurile acestora, durata, destinația exactă, dimensiunea atacului și ulterior motivul. Cu siguranță, România poate diminua prin surse și forțe proprii această aparentă stare de criză nonviolentă în raport cu Rusia sau disputele cu Ungaria. Ținând cont de actualul context geopolitic și poziția geostrategică a României în

1. Cătălina Todor, „The topicality of security dilemma's spiral model in analysing the international environment", în *Strategic Impact*, Vol.63, Nr. 2, "Carol I" National Defence University Publishing House, București, 2017, p.25.

calitate de aliat NATO, aceasta nu are competența și puterea necesară în a dizolva o astfel de criză, fie aceasta chiar și una nonviolentă.

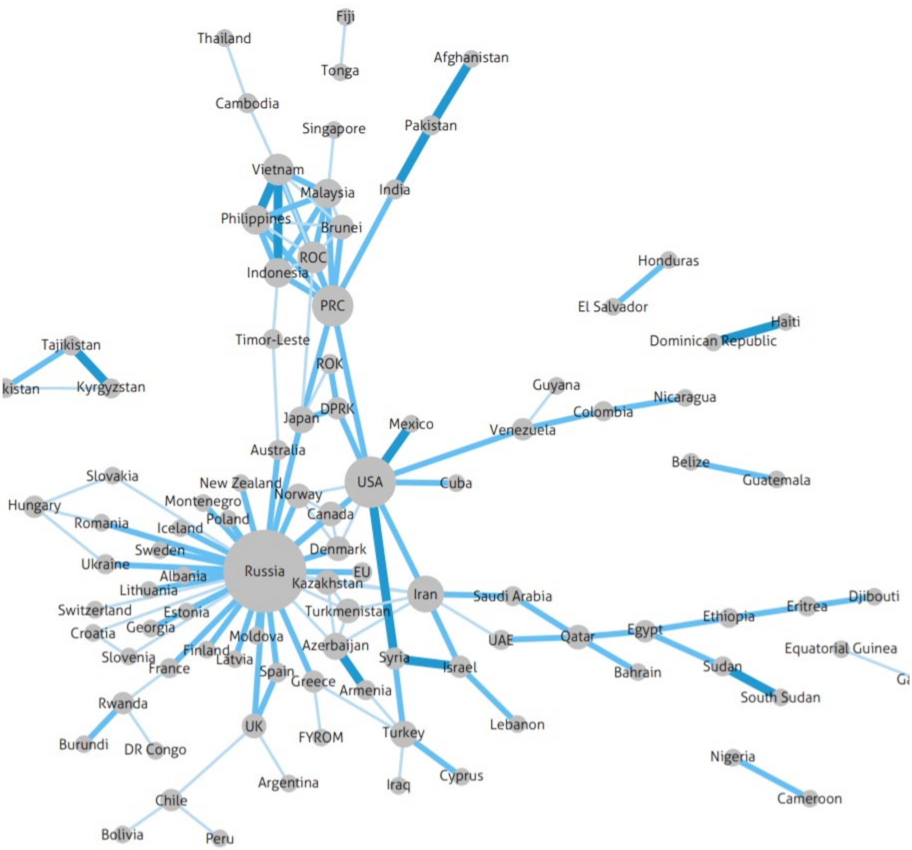


Figura nr.17. Raportul anual privind conflictele la nivel global *„Global Conflict Panorama, Interstate Conflict Constellations 2012, 2014, and 2017"*[1]

Reflectând asupra celor două perspective prezentate în Figura nr.17. și Figura nr.18., anume conflictul în sectorul cibernetic și conflic-

1. Heidelberg Institute for International Conflict Research, Conflict Barometer 2017, „Global Conflict Panorama: Interstate Conflict Constellations 2012, 2014, and 2017", p.19, https://hiik.de/conflict-barometer/current-version/?lang=en, accesat în data de 09.12.2018.

tul în forma sa tradițională (*armat, politic șamd.*) și identificând modelul care se regăsește în cele două hărți relaționale mai sus prezentate, observăm realități care au la bază aceleași principii ale realismului în forma sa cea mai pură.

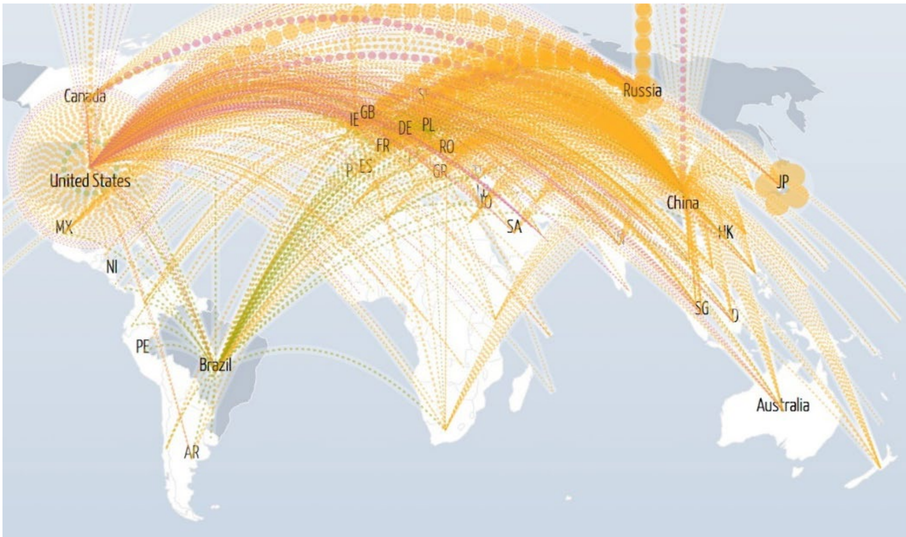


Figura nr.18: *Simulare în timp real a ~1% din atacurile de tip DDOS la nivel global, „Digital Attack Map" din data de 22 septembrie 2018, ora 18:00*[1]

În urma unei analize introspecte asupra sistemului de securitate național, cu implicații în și din sectorul cibernetic, statele aduc în ecuație nevoia de a identifica soluții ofensive și defensive, în situații ipotetic impuse de amenințările de la granițele „teritoriale" ale acestora. În acest context, dilema de securitate este dată de nevoia practică de a înțelege nivelul de insecuritate sau securitate într-un mediu scalabil și oarecum tangibil al statelor, raportat la amenințările și vulnerabilitatea acestora în toate sectoarele de securitate.

De ce spirală de securitate și nu doar o simplă dilemă? Diferența este dată de escaladarea insecurității de la o situație devenită mai

1. Google Ideas. DDoS data ©2013, Arbor Networks, Inc., http://www.digitalattackmap.com/#anim=1&color=0&country=RO&list=0&time=17796&view=map, accesat în data de 09.12.2018.

târziu o problemă și în cele din urmă o dilemă cu „iz" de conflict. Prin utilizarea modelului spiralei de securitate, putem înțelege și chiar prognoza rezultate bazate pe escaladarea insecurității și raportul pe întregul parcurs dintre elementul de securizat și factorii externi de influență. Se pot simula soluții, traiectorii, rezultate ale acțiunilor defensive, neutre ori ofensive. O particularitate a „dilemei de securitate" este dată de o lipsă a unei ecuații de calcul a acesteia, precum se poate calcula riscul sau gradul de vulnerabilitate.

În calitate de cadre de analiză a dilemei de securitate în forma sa generală, am identificat un număr de trei perspective concludente, anume:

A. *Teoria realismul ofensiv* este o teorie a maximizării puterii de stat prin mijloace și scopuri oportuniste[1]. Statele căutându-și mereu resursele necesare în vederea maximizării puterii vor face aproape orice pentru a-și asigura în acest context internațional atât securitatea cât și integritatea, opunându-se cu tărie sistemelor anarhice, care fac presiuni asupra acestora din ambele medii, atât din cel interior cât și din cel exterior. Teoria realismului ofensiv este în aceeași măsură descriptivă, reprezentând modul în care statele au acționat în trecut, cât și prescriptivă, sugerând sau prognozând modul în care statele ar trebui să conducă în zona de politică externă. Susținători ai teoriei realismului ofensiv sunt cercetători din sectorul relațiilor internaționale, personalități precum Gilpin R., Liberman P., Schweller R.L., Labs E.J., Zakaria F., Mearsheimer J.J., Elman C.

B. Susținătorii teoriei *realismului defensiv* susțin că sistemul internațional încurajează statele să urmeze un comportament moderat și limitat pentru a-și asigura supraviețuirea și siguranța, promovând extinderea (deloc ofensivă) în cazuri

1. Brandon Valeriano, „The Tragedy of Offensive Realism: Testing Aggressive Power Politics Models", în *International Interactions*, Vol. 35, Nr. 2, Edit. Routledge Taylor&Francis Group, Londra, 2009, p.180.

și situații cu totul speciale. Rațiunea care stă la baza acestei teorii este dată de ipoteza prin care maximizarea puterii unui stat, pentru asigurarea unui grad acceptabil de securitate prin mijloace bazate pe agresiune, concurență și extindere, este neproductivă, deoarece va provoca diverse dileme de securitate și contrabalans nefavorabil și, astfel, va limita, dacă nu chiar împiedica efortul statului de a-și spori securitatea în relație și raport cu ceilalți actori statali și non statali. Reprezentanții și susținătorii acestei teorii sunt experți și cercetători politici, precum Christopher Layne, care-și exprimă certitudinea asupra acestei teorii pornind de la premisa potrivit căreia „statele echilibrează împotriva hegemonilor”[1]. Pentru realiștii defensivi, sistemul internațional oferă rareori motive pentru o posibilă și necesară expansiune prin asigurarea unui echilibru militar ofensiv-defensiv de ordin geografic sau de ordin patologic, reprezentat de credința, convingerile, percepțiile elitelor de guvernare ori coalițiilor care să explice supra expansiunea, sub-echilibrarea, îngrădirea și supra extinderea[2]. Joseph Grieco a patentat termenul *„poziționaliști defensivi”* în lucrarea sa *„Cooperarea între Națiuni”*, unde a și redat poziția susținătorilor realismului pozițional sau defensiv prin afirmarea faptului că securitatea este autosuficientă. Marile puteri caută să-și maximizeze securitatea prin păstrarea echilibrului de putere existent, de cele mai multe ori printr-o varietate de strategii defensive. Acești susținători ai teoriei realismului defensiv sunt de asemenea cercetători politici și de securitate în sectorul relațiilor internaționale, personalități precum Jervis,

1. Christopher Layne, „The Unipolar Illusion: Why New Great Powers Will Rise”, în *International Security*, Vol. 17, Nr. 4, Massachuset, Edit. MIT Press, Massachuset,1993, pp.7,45.
2. J.W. Taliaferro, „Security Seeking under Anarchy: Defensive Realism Revisited”, în *International Security*, Vol. 25, Nr. 3, Massachusetts, 2000, pp.128–161, https://www.mitpressjournals.org/doi/10.1162/016228800560543, accesat în data de 20.12.2018.

R., Waltz, K.N., Posen, B.R., Walt, S.M., Grieco, J.M., Snyder, J., Glaser, C.L., Layne, C., Van Evera, S.

C. *Realismul Bayesian* vine ca o a treia soluție la încercarea de soluționare a dilemei de securitate sau de destructurare a spiralei de securitate prin cele două școli de gândire ale realismului structurat, realismul defensiv și realismul ofensiv, ale cărui inițiator a fost Waltz și care a contribuit semnificativ la înțelegerea relațiilor internaționale și încrederii în acest sector[1]. Aceasta este o teorie pe care Andrew H. Kydd o poziționează ca o posibila alternativă la realismul ofensiv sau cel defensiv. În această nouă abordare, realismul Bayesian pornește de la prezumția că statul este un actor unitar și rațional care se bazează pe o relație și un raport între analiza teoretică a convingerilor și comportamentelor descrise de teoria Bayesiană a schimbării convingerilor. Statele au preferințe diferite pentru revizuirea *status quo-ului*, iar nivelul de încredere între ele este variabil, spre deosebire de realismul ofensiv și defensiv în care statele sunt mereu în căutare de securitate. Altfel spus, în terminologia utilizată de dezbaterea subiectului inter-realist, abordarea acestei noi teorii este necesară pentru a găsi o cale de mijloc între abordarea concentrată pe realismul neoclasic sau neorealismului îmbrățișat de statele cu diferite obiective, motivații sau viziuni privind securitatea și realismul defensiv, care este adoptat de state care se concentrează pe semnalarea motivației de securitate. Folosind un cadru de semnalizare, Andrew H. Kydd arată că statele cu credit și vot de încredere pot fi susceptibile de detașarea față de cele partenere, adoptând o agendă dublă, și totodată arată cum într-un cadru dinamic statele raționale pot folosi metode costisitoare pentru a reduce neîncrederea și de a o aduce la un nivel ușor de

1. Andrew H. Kydd, *Trust and mistrust in international relations*, Edit. Princeton University Press, Princeton, New Jersey, SUA, 2005, p.13.

gestionat, uneori chiar și indiferent de costuri, totul pentru a începe o relaționare eficientă[1].

	Motivația statelor	Grad de încredere
Realism ofensiv	Securitate	Scăzut
Realism defensiv	Securitate	Variabil
Realism Bayesian	Mixt	Variabil

Tabelul nr.5. Viziune asupra raportului anarhie-încredere din prisma celor trei școli de gândire[2]

III.1.11. Teoretizarea balanței ofensiv-defensiv în sectorul cibernetic

Fie că vorbim de securitate națională sau de securitate internațională, un lucru este cert, atuurile ofensivei în sectorul cibernetic devansează rapid încercarea sistemelor defensive de a asigura un obiectiv sigur. Din perspectiva statelor, sistemele ofensive sunt evidențiate de minimul de resurse necesare, de ușurința cu care aceste strategii pot fi concepute, realizate și menținute, precum și de costurile relativ scăzute care stau în spatele acestora. În aceeași măsură, eficiența este dată de atingerea rezultatului propus prin obiectivele strategice și operaționale cu un minim de daune colaterale[3]. Dacă o strategie defensivă se construiește și se aplică pe un areal întins, precum o rețea de comunicații voce/date, strategiile ofensive sunt orientate punctual, oportunist bazate pe certe vulnerabilități, cu un scop concret și un obiectiv clar. Mai mult de atât, diferența esențială de resurse, precum timpul, este critică. Astfel dacă un atac din partea unui stat asupra unei ținte exacte de importanță națională a unui stat rival se poate

1. Avidit Acharya, Kristopher W. Ramsay, "The Calculus of the Security Dilemma", în *Quarterly Journal of Political Science,* Vol. 8, nr. 2, Princeton, USA, 2013, pp. 184-185, http://stanford.edu/~avidit/security.pdf, accesat în data de 20.12.2018.
2. Andrew H. Kydd, *op.cit.*, p.14.
3. Lieber Keir, Cyber Analogies, „The Offense-Defense Balance and Cyber Warfare", în *Cyber Analogies*, Institutional Archive of the Naval Postgraduate School, Monterey 2014, p.96, http://hdl.handle.net/10945/40037, accesat în data de 29.12.2018.

executa instant sau, în funcție de complexitatea operațiunii, atacurile pot fi executate într-un interval de ordinul minutelor, timpul necesar identificării intruziunii și daunelor ori a altor implicații printr-un sistem defensiv este de ordinul zecilor de minute, orelor sau chiar zilelor. Motivat de acest nou areal sau teatru de operațiuni virtual, în sectoare precum cel militar, cel al culegerii de informații, s-a recurs la diverse modele de securitate (ofensive / defensive), având la bază un sistem de comandă și control al operațiunilor de securitate cibernetică care sunt interdependente de tehnologia informației. Sumarizând și sintetizând într-o formulă simplificată scopul acestora, înțelegem că totul s-ar rezuma la *nevoia de supremație cibernetică pentru împlinirea securității naționale*. Aceasta se bazează pe o altă dilemă de securitate cunoscută ca (ODT) „*teoria balanței ofensiv-defensiv*", care a apărut natural ca explicație la cursa înarmărilor nucleare, dar care, în acest context, este folosită de susținătorii realismului defensiv pentru a explica de ce motivațiile *status quo-ului* sunt uneori utilizate ca o pârghie care duce la un inevitabil conflict, uneori chiar armat, postulând că atunci când tehnologia militară predominantă favorizează ofensiva asupra operațiunilor defensive, gradul de probabilitate în apariția unui conflict crește proporțional cu raportul dintre puterea ofensivă a unui stat și cea defensivă a unui alt stat rival.

Gândirea dominantă în sistemul internațional, așa cum susține Jervis, este dată de o afirmație cu iz ofensiv, care poate îmbrăca diverse forme, dar care are un singur înțeles, acela că „*este mai ușor să distrugi armata unui stat și să-i ocupi teritoriul decât să-ți aperi propriile teritorii*" (o gândire care stă la baza multor strategii adoptate de Rusia în ultimii 100 ani). Gândirea cu motivație defensivă și de apărare este dominantă numai atunci când unei țări îi „*este mai ușor să-și protejeze și să dețină teritoriile intacte și protejate, securizate, decât să avanseze în cucerirea unor noi teritorii, prin distrugere și ocupare militară*". Teoria balanței ofensivă-defensivă a ajuns, în ultimele trei decenii, să ocupe un loc principal în dezvoltarea relațiilor internaționale, dar și în

analiza politicii externe. Cercetătorii au folosit teoria pentru a lansa o gamă largă de aspecte teoretice și de problematici privind sectorul politic, incluzând analiza comportamentului alianțelor, doctrina militară, concurența și cooperarea militară, strategia și politica nucleară, precum și controlul armelor convenționale[1].

Când avantajul se află de partea atacatorilor, marile puteri sunt puternic provocate în a-și spori capacitățile ofensive și în a căuta modalități de expansiune teritorială sau a puterii prin noi alianțe strategice, cu scopul de a-și consolida poziția, altfel riscând să se identifice într-o poziție defensivă, ceea ce nu este de dorit, deoarece presiunea și riscul de a fi atacate sunt iminente. Se consideră că factorii dați de evoluția tehnologică definesc balanța de apărare-eficiență și oferă noi perspective.

De exemplu, specialiștii consideră că tehnologiile de îmbunătățire a mobilității în cele cinci mari arealuri (*terestru, maritim, aerian, cibernetic și cosmic*) favorizează atacatorii, în timp ce tehnologiile care sporesc și optimizează puterea de foc întăresc sectorul de apărare, făcându-l mai eficient. Teoria a fost pusă în aplicare pentru a defini posibilele debuturi ale conflictelor sau absența războaielor în cursul istoriei. Se poate exemplifica o astfel de aplicare a teoriei pe parcursul Primului Război Mondial, în care evoluția, cercetarea și inovarea armelor de foc mici, precum și a artileriei au creat o tendință care, deși greșită, a fost larg răspândită și îmbrățișată de cei mai mulți lideri și elite europene în „*cultul ofensivei militare*". Astfel, au fost încurajați să lanseze războaie premature, slab fundamentate și sub eticheta prevenției în ceea ce privește un risc greu de asumat și iminent. După cum a demonstrat-o războiul de tranșee, încă de la începutul „revoluției" armelor de foc, în realitate tehnologia și dezvoltarea tehnologică a

1. Charles L. Glaser, Chaim Kaufmann, „What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics)", în *International Security*, Vol. 22, nr. 4, Massachusetts, 1998, p.44, https://web.stanford.edu/class/polisci211z/2.1/Glaser%20%26%20Kaufmann%20IS%201988.pdf, accesat în data de 29.12.2018.

armelor a favorizat în mare măsură sectorul defensiv, cel de apărare militar. Teoria a fost însă aspru criticată atât pentru logica defectuoasă, cât și pentru lipsa de parcimonie. Mai critic, în ceea ce privește nevoia de a explica conflictul interstatal prin prisma acestei teorii, îi este demonstrată lipsa de sprijin empiric. Se constată că balanța ofensiv-defensiv reală sau cea percepută în contextul războiului sau conflictului militar nu este un predictor statistic semnificativ[1].

Teoria balanței ofensiv-defensive s-a reconceptualizat în mod absolut natural datorită apariției acestui nou areal, unde aplicabilitatea acestei teorii a fost posibilă. Reconceptualizarea s-a datorat, în mod deosebit, naturii non-teritoriale a tehnologiilor cibernetice versatile și bazate pe liniile de cod binar în detrimentul muniției de foc, lucru care înlocuiește cu succes nevoia de mobilitate și capacitatea armelor de foc din celelalte patru spații reale.

III.2. Supranaționalism

Cu toate că nu identificăm termenul „supranaționalism" în dicționarul limbii române, acesta este necesar pentru a numi ideologia pusă în practică fără rezerve la nivel internațional de uniuni internaționale, precum Uniunea Europeană, prin entități, precum cele două mari organisme, Parlamentul European și Consiliul Europei. Una dintre definițiile termenului ar putea fi extrasă din însuși compoziția termenului „supra" și „național". În contextul științelor relațiilor internaționale îl putem defini într-o formă brută, ca un adjectiv ce reflectă ceva dincolo de autoritatea sau jurisdicția unui guvern național și îi putem identifica rolul prin definirea atribuțiilor instituțiilor supranaționale ale Uniunii Europene.

1. Gortzak Yoav, Haftel Z. Yoram, Kevin Sweeney, "Offense-Defense Theory: An Empirical Assessment", în *Journal of Conflict Resolution*, Vol. 49, Nr. 1, Edit. Sage Publications, Inc., Ohio, SUA, 2005, pp.67–89, https://journals.sagepub.com/doi/abs/10.1177/0022002704271280, accesat în data de 23.12.2018.

Înțelegerea termenului supranațional ca fiind o ideologie opusă realismului este, în viziunea autorului tezei, una total eronată și lipsită de fundament rațional. Organismelor supranaționale le sunt date puteri sporite și autoritate asupra unor certe aspecte ale uniunii și statelor membre ale acestor uniuni, dar nu trebuie să omitem scopul și obiectivele pentru care aceste state au aderat la aceste uniuni. „*Prin forțele proprii, statele, cu siguranță nu ar putea trata anumite problematici sau cu atât mai mult nu le-ar putea gestiona eficient sau administra în condițiile progresiste ale uniunilor precum este cazul Uniunii Europene sau precum este modelul de dorit al Statelor Unite ale Americii. În cazul României, care are calitate de țară membră a Uniunii Europene, putem afirma faptul că strategia și procesul de construcție europeană se bazează sau chiar începe cu întărirea suveranității naționale. Oricare ar fi acela, proiectul național în nici un caz nu se poate opune proiectului european*”[1].

Termenul „Federație” poate fi înțeles ca „*o uniune de state a cărei autoritate provine de la cetățenii ei și este rezultatul unei construcții supreme; toate puterile își derivă autoritatea din aceasta. În plus, guvernul central are controlul asupra unor domenii importante, precum apărarea, politica externă, moneda comună și taxele generale. Este, de asemenea, expresia alegerilor generale care au loc pe întreg teritoriul federației. Cele mai cunoscute exemple de federații sunt Statele Unite după 1789, Elveția după 1984, Uniunea Sovietică, Federația Rusă, fosta Iugoslavie etc.*

Dacă facem o scurtă analiză a UE, plecând de la premisele anterioare, putem spune că aceasta este o organizație supranațională care are elemente con-federaliste (tratate, un Consiliu de Miniștri, care deține puteri legislative și decizionale, Consiliul, principala autoritate politică, regula unanimității în procesul de luare a deciziilor) cele federale (cetățenia comună, moneda unică, primatul dreptului Uniunii față de legea statelor membre, instituțiile supranaționale etc.).

1. Prelegere susținută de prof. univ.dr Adrian Liviu-Ivan în cadrul conferinței „*O Europă mai sigură*”, Universitatea din Oradea, Oradea, 15.01.2019.

Pentru a deveni un stat federal, Uniunea Europeană are nevoie de o Constituție."[1]

Formându-se această federație de state apare Uniunea Europeană, care subit este înzestrată cu întreg arsenalul organismului supranațional.

Putem astfel exemplifica schimbarea paradigmei de securitate prin înțelegerea schimbărilor apărute la nivel militar internațional. Până nu de mult, *„la nivel aliat, sfârşitul Războiului Rece găsea armatele NATO pregătite să înfrunte doar adversari convenționali, instrumentele de intelligence militar folosite în acest sens având o dezvoltare preponderent tehnică, orientată cu precădere împotriva unor forțe combatante manevrier"*[2]. De asemenea, subliniem faptul că activitatea de culegere de informații și intelligence militar nu beneficiază de experiența cooperărilor în plan operațional cu instituțiile naționale ale statelor membre (*ex. de combatere a terorismului*), datorită rigidității legislației naționale în domeniu. În acest context, s-a constatat o nouă necesitate, controversată de altfel, identificarea de soluții pentru înțelegerea unui mediu operațional complet necunoscut, cel cibernetic. *„Organizarea de tip coaliție a impus adaptări care să permită schimbul rapid de informații atât între națiuni, categorii de forțe sau agenții cât şi între eșaloanele tactic-operative şi strategice ale fiecărei țări participante. Identificarea soluțiilor pentru schimbul de informații a determinat în final o schimbare completă de paradigmă în domeniul clasificării informațiilor, respectiv de la limitarea accesului pe baza necesității de a cunoaște (need to know) la diseminarea automatizată a informațiilor în interiorul comunității"*[3]. În acest nou context, trebuie analizate și redefinite componentele funcționale atribuite anterior unor structuri cu specific militar, precum:

---

1. Ivan Adrian-Liviu, „Governance and "European Constitution", în *Transylvanian Review of Administrative Sciences*, Vol.4, nr.22, 2008, p.79, http://rtsa.ro/tras/index.php/tras/article/view/382/372, accesat în data de 30.04.2019.
2. Zavate Cristian, „Angajarea țintelor teroriste. Exemplul frontului", în *Intelligence*, Nr. 36, București, 2018, p.78.
3. *Ibidem*, p.79.

mobilitatea şi manevra, factorii de protecție și sprijin de foc, logistica și intelligence, comandă şi control. Așadar, instrumentele procesului de gestionare a întregului ciclu de viață a informației solicită, din partea sectorului militar și public/civil, o nouă organizare, într-un mod matematic, algoritmic și foarte bine structurat în relație de interdependență cu mediul cibernetic. Aceasta a dus la implementarea unor sisteme de prelucrarea automatizată şi gestionare a unor volume mari de date. Utilizarea rețelelor a devenit absolut necesară, iar acest fapt a făcut ca aceasta să fie principala modalitate de apelare și gestionare a informațiilor existente în bazele de date secretizate. La nivelul NATO, o mare parte a sistemelor informaționale, rețelelor și sistemelor de baze de date specifice componentei de intelligence militar s-au constituit într-o platformă de profil, parte integrantă a arhitecturii rețelei NATO SECRET, Intelligence Functional Service (INTEL-FS). Și-au făcut apariția, în mod natural, aplicațiile specifice de tipul client-server (Analist Notebook i2[1]), care au adus un aport considerabil în OSINT, SIGINT sau GEOINT[2], schimbul informațional fiind posibil azi în timp real din orice zonă a mapamondului.

Analiza NATO, prin componenta sa NCI cu privire la inițiativa JISR, arată în contextul mai sus menționat că statele membre pot fi pregătite împreună pentru întâmpinarea unui război hibrid sau asimetric cu toate provocările pe care acestea le-ar putea aduce. Succesul statelor de această dată stă în implementarea unui set de standarde, protocoale, procese și sisteme naționale agreate de toți aliații. Provocările, cărora statele singure nu le-ar putea face față indiferent de puterea economică sau capacitatea militară, sunt date chiar de volumul de date și complexitatea acestora, de capacitățile

1. IBM i2 Analyst's Notebook Release Notes, https://www-01.ibm.com/support/docview.wss?uid=swg27036288, accesat în data de 12.02.2019.
2. The NATO Core Geographic Services System, „Enterprise GIS for Defense Provides Strong, Centralized
Geospatial Capabilities", ArcGIS 3D Analyst, ESRI, 2014, https://www.esri.com/library/brochures/pdfs/nato.pdf, accesat în data de 12.02.2019.

necesare de stocare și analiză, dar nu în ultimul rând de „promisiunile” inteligenței artificiale[1]. Operațiuni de tip coaliție în țările aliate sau în țările care reprezintă un oarecare interes economic şi existența la nivelul acestora a unor structuri de informații mature și dinamic construite fac să apară într-un mod deloc artificial un parteneriat eficient alături de diverse ONG-uri de profil sau think-thank-uri, care oferă serviciilor de informații interne și externe posibilitatea de a participa activ alături de structuri militare, dar şi de alte servicii partenere ori structuri de profil în asigurarea securității naționale.

Putem înțelege din acest exemplu, succint expus, faptul că statele își pot păstra autonomia și suveranitatea asupra acțiunilor și resurselor proprii (*din care fac parte și informațiile*) prin participarea activă a acestora în frontul comun al statelor aliate pentru protejarea alianței. Supranaționalismul se manifestă în acest caz într-o oarecare formă forțat conjuncturală, reprezentat fiind de puterea nu a unui stat, ci a unei coaliții materializate printr-un tratat pentru asigurarea securității teritoriale. Adoptarea unei strategii bazate pe principiul realismului ar putea periclita nu doar poziția statului, ci și securitatea acestuia în raport cu activitatea celorlalte state față de posibilii adversari.

În acest context, suveranitatea nu ia o formă distinctă, aceasta se referă la deținerea autorității exclusive asupra unui domeniu, fie că acesta este unul real sau unul virtual, cu condiția ca acesta să fie clar delimitat într-o formă recunoscută și de actorii internaționali de securitate implicați. În ceea ce privește securitatea internațională, termenul este adesea asimilat suveranității statale și problemelor asimilate chestiunii suveranității. *„Acest concept a apărut în Europa secolelor XVI și XVII și a fost cuprins în dreptul internațional prin Tratatul de la Westfalia, din 1648, unde tratatul a stabilit principiul că poli-*

1. Kurt Veum , NATO NCI, „Joint Intelligence, Surveillance & Reconnaissance (JISR) in NATO”, https://fmv.se/Global/Dokument/Nyheter%20och%20Press/2016/Sensorsymposium%202016/2_Veum_NVIA_JISR%20Initiative%20-%20Overview%20for%20SWE%20Sensors%20Conf%20(7%20Sep%202016)%20N-U.pdf, accesat în data de 12.02.2019.

tica internă a fiecărui stat este propria afacere și că neînțelegerile asupra problemelor interne ale altui stat nu constituie motive întemeiate pentru o intervenție[1]. Acest Tratat reprezintă o realitate și o nevoie care a fost materializată, primind și caracter legislativ ulterior. O altă realitate este cea a suveranității statului națiune asupra problemelor interne și a efectelor produse de politicile și măsurile luate de acesta în raport cu atingerea suveranității unui alt stat, ecuație în care apare necesitatea unui dialog diplomatic imparțial între principiile realismului și ale supranaționalismului cu un scop comun - *„Pax sit christiana, universalis, perpetua veraque et sincere amicitia !“*

În extinderea CE și a UE se poate observa că „în cazul țărilor AELS, teoria cea mai adecvată a fost raționalismul instituționalist." Regatul Unit al Marii Britanii, Austria, Danemarca, Finlanda și Suedia au inițiat, prin intermediul CE sau UE, proiecte cu scopul ultim de a prospera din punct de vedere economic și de a-și întări poziția de securitate, pe când în procesul de extindere al Europei Centrale și de Est ideologia a fost una bazată pe constructivism, cu atât mai mult cu cât statele care își doreau aderarea aveau ca obiectiv principal renunțarea la stigmatul adus de „identitatea estică" și își doreau întoarcerea la o Uniune Europeană. Totodată, UE își afirma vădit preferințele cu privire la interdependențele economice și geopolitice date de proximitatea geografică a Europei Centrale și de Est sau de competiția privind accesul la piețele celorlalte state, investițiile și sporirea bugetelor naționale printr-o structură economică competitivă, dinamică și unitară.[2]

Uitându-ne la contextul istoric, vom observa că tratarea subiectului suveranității într-o perioadă a dezbaterilor europene între interguvernamentalism și supranaționalism pentru România a fost una

1. Paul Robinson, *op.cit.*, pp.220-221.
2. Adrian Liviu-Ivan, „Constructivismul și Integrarea Europeană: Contribuții și Limite" în *Hello World!: Contemporaneitate și provocările globalizării*, Edit. CA Publishing, Cluj-Napoca, 2014, p.146.

fragilă. Sensibilitatea, încă de la început, a fost dată de complexitatea fenomenului de transfer al suveranității din partea statelor doritoare să adere la noua construcție Europeană, care nu era foarte bine înțeles. Dacă în urmă cu mai bine de 20 de ani, pentru foarte mulți politicieni români din acea perioadă, aderarea României la noua construcție Europeană prin acceptarea în Consiliul Europei sau în OSCE, aderarea la NATO şi integrarea în UE, erau noțiuni greu digerabile[1], astăzi asistăm la un nou set de aspirații și o viziune proaspătă. Unul dintre imboldurile primite de România este și încrederea primită din partea statelor membre și a întregii UE pentru a deține, în 2019, Președinția Uniunii Europene.

Cu alte cuvinte, este de-a dreptul fascinant de observat tranziția de la forma inflexibilă de guvernământ - de dinaintea alipirii României la UE, la capacitatea de adoptare a fenomenului globalizării și ușoara flexibilitate în transferul controlat al suveranității naționale în scopuri reale și care primează statului.

Astfel, *„aderarea statelor din Europa Centrală şi de Est la Uniunea Europeană s-a fundamentat, în primul rând, pe principiul „reîntoarcerii în Europa", având din acest punct de vedere o dimensiune cultural-identitară evidentă. Cu toate acestea, nu pot fi neglijate componentele logico-realiste privind necesitățile economice şi geopolitice (mai ales de securitate) ale acestor state"*[2].

Aceste două ideologii, realismul și supranaționalismul vor sta în permanență pe masa factorului de decizie și vor influența acțiunile statelor în raport cu păstrarea securității naționale sau progresul în plan internațional.

În ceea ce privește Statul Român, acesta a dorit și a reușit în mare parte să obțină avantaje geopolitice, geostrategice și economice prin integrarea sa în structuri organizaționale supranaționale şi guverna-

1. Ivan Adrian-Liviu, *Statele Unite ale Europei: Uniunea Europeană între interguvernamentalism şi supranaţionalism*, Editura Institutul European Iaşi, Iași, 2007, p.330.
2. *Ibidem*, p.339.

mentale internaționale care pot să garanteze un grad de securitate corespunzător, dacă nu optim. Acest lucru nu face altceva decât să ne confirme direcția aleasă de statul român, anume Calea Europeană, o cale a Europei Unite a Națiunilor, prin abordarea unei viziuni lărgite și adoptarea unei ideologii supranaționaliste cu o formă de guvernământ elitistă.

III.2.1. Supranaționalism și securitate cibernetică

Putem afirma că evenimentul care stă la baza evoluției României în domeniul securității cibernetice este participarea acesteia la conferința interguvernamentală bilaterală organizată în contextul negocierilor UE cu state precum România, Slovacia, Letonia, Bulgaria şi Malta, în perioada 10-11 decembrie 1999, eveniment care s-a desfășurat la Helsinki, fiind organizat de către Consiliul European. În urma aceste conferințe, președintele Romano Prodi, în baza viziunii sale privind relansarea integrării europene, s-a arătat mult mai receptiv la problemele Europei Centrale şi de Est. În urma deschiderii negocierilor din partea UE (din 16 februarie 2000), la 26 mai 2000, Guvernul României a și încheiat discuțiile privind dezvoltarea întreprinderilor mici şi mijlocii (SMB), știință, cercetare și inovare, educație, formare profesională şi tineret, relații internaționale, politică externă şi de securitate comună, unde era cuprinsă, într-o formă incipientă, și securitatea sectorului cibernetic.

Odată cu lărgirea spațiului UE, s-a acordat o atenție sporită şi politicii economice, dreptului comunitar, ocupării forței de muncă și modernizării. Așadar, a fost lansat un set de Programe-cadru pentru cercetare şi dezvoltare tehnologică în cadrul căruia s-au adoptat noile programe educaționale şi de formare profesională. A existat un real interes pentru crearea unei societăți a cunoașterii, a unei societăți a informației. Comisia a lansat inițiativa e-Europe privind ameliorarea accesului cetățenilor la informare. Așadar, Parlamentul European şi

Consiliul de Miniștri au adoptat texte legislative de utilizare a Internetului şi s-a decis dezvoltarea unui sistem european de navigare prin satelit, intitulat Galileo[1].

La 15 ani după identificarea acestor noi resurse, facil de utilizat în contextul politic, economic, militar, de intelligence, diplomatic șamd., dezvoltarea tehnologiei informației și comunicațiilor a creat o nouă dimensiune a securității informațiilor. Sectorul financiar, sectorul sănătății, cel energetic și cel al transporturilor sunt doar câteva dintre domeniile care se bazează din ce în ce mai mult pe tehnologia informației și a comunicațiilor[2]. Cu toate acestea, pot apărea probleme atunci când această tehnologie este conectată la o vastă rețea de calculatoare sau echipamente, devenind o rețea IoT care devine accesibilă terților actori de securitate rău intenționați. Spre exemplu, Tesco Bank a devenit victima atacatorilor cibernetici în 2016, aceștia reușind să înfăptuiască unul dintre cele mai mari atacuri cibernetice din Europa până la acea dată, producând pagube de 2.26 milioane £, iar Tesco Bank a fost obligată la plata a 16.4 milioane £[3]. Acest atac a avut ca obiectiv extragerea de fonduri din conturile bancare, drept urmare 20.000 de conturi au fost afectate[4]. Acest exemplu este unul dintre nenumăratele cazuri apărute în ultimii cinci ani. Organizațiile vizate au fost cele din industria producătoare de mașini (cazul atacu-

---

1. *Ibidem*, pp.194-195.
2. Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions – „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accesat în data de 13.02.2019
3. The Guardian Press Association, „Tesco Bank fined £16.4m by watchdog over cyber-attack", https://www.theguardian.com/business/2018/oct/01/tesco-bank-fined-cyber-attack-fca, accesat în data de 13.02.2019;
4. Ben Martin, James Titcomb, „Regulators could fine Tesco Bank over cyber attack", 07.11.2016, https://www.telegraph.co.uk/business/2016/11/07/tesco-bank-to-freeze-customer-transactions-after-hacking-attack/, accesat în data de 13.02.2019.

lui de la Mioveni - Grup Renault[1]), băncilor[2] și instituțiilor medicale[3] sau furnizorilor de infrastructuri critice, ceea ce ridică nivelul de risc la o amenințare clară pentru interesele pieței UE și pentru viața privată a cetățenilor.

Experții și strategii în domeniul securității informatice sunt de acord că infrastructurile critice și sistemele de comandă și control din sectorul industrial / SCADA reprezintă, din perspectivă economică, coloana vertebrală a oricărei țări moderne sau contemporane. Grupări de activiști profesioniști în mediul cibernetic și chiar unele state, prin structurile lor specializate, s-au concentrat pe atacurile infrastructurilor critice pentru a le sabota, dezafecta sau în unele cazuri de a le neutraliza. Un astfel de caz a fost identificat în cursul anului 2018, când serviciile de informații israeliene, cu ajutorul unui program malițios similar Stuxnet, dar mult mai complex, au extras date privind infrastructura critică și nucleară a Iranului, tocmai cu ajutorul telefonului mobil al președintelui Hassan Rouhani[4]. Cu această ocazie, au fost expuse atât locația arhivelor nucleare, cât și a depozitelor de materiale nucleare[5] în fața Adunării Generale a Națiunilor Unite din 27 septembrie 2018[6].

1. Ovidiu Posirca, „Dacia production in Romania, partially crippled by cyber-attack | WannaCry infection suspected", 13.05.2017, http://business-review.eu/news/dacia-production-in-romania-partially-crippled-by-cyber-attack-wannacry-infection-suspected-137678, accesat în data de 13.02.2019.
2. David Bond, „Seven UK banks targeted by co-ordinated cyber attack", 25.04.2018, https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb, accesat în data de 14.02.2019.
3. Matthew Field, 11.10.2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/, accesat în data de 14.02.2019.
4. Toi Staff, „TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet", 31.10.2018, https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/, accesat în data de 14.02.2019.
5. Michael Bachner, Toi Staff, At UN, „Netanyahu reveals Iranian nuclear warehouse, urges IAEA to go inspect it", https://www.timesofisrael.com/netanyahu-reveals-secret-iranian-nuclear-warehouse-in-un-speech/, accesat în data de 14.02.2019;
6. Consiliul European, Consiliul Europei, „Adunarea Generală a ONU, New York, 27/09/2018", https://www.consilium.europa.eu/ro/meetings/international-sum-

În mod tradițional, sistemele de control au fost segregate de zonele nesecurizate, cum ar fi rețelele publice sau private din sectorul comercial.

III.2.2. Istoricul atacurilor cibernetice

Pentru a putea înțelege nevoia de a guverna un anumit spațiu sau domeniu, consider necesară cunoașterea acestuia și cum poate fi cunoscut mai bine dacă nu prin întocmirea unui itinerar, istoric chiar, sau a unui traseu al evenimentelor care au adus această nevoie de a guverna spațiul sau domeniul în care acestea s-au desfășurat și încă se propagă.

Astfel, primul atac mediatizat, suspectat a fi un atac cibernetic asupra infrastructurii critice industriale a fost în 1982[1], când conducta de gaz Trans-Siberiană a explodat și se presupune că explozia a fost provocată de un troian activat prin instalarea acestuia la sistemul de control.

Stuxnet, un alt vierme informatic cu capacități extraordinare, descoperit în 2010, a reușit să infecteze cele mai securizate instalații nucleare iraniene cu ajutorul unui dispozitiv fizic - unitate de memorie externă de tipul flash-drive USB. Prin intermediul acestui vierme informatic instalat, s-a reușit modificarea parametrilor de viteză ai motoarelor reactoarelor nucleare. În urma unei analize de detaliu, reiese faptul că o dată cu o cunoaștere a echipamentelor și tehnologiilor utilizate, chiar și în zilele de azi, se pot crea soluții potrivite și croite pe nevoile exacte ale atacatorului[2].

Atacurile cibernetice directionate spre infrastructurile critice primesc creditul și valoarea acestora sau a resurselor, respectiv a

mit/2018/09/27/, accest în data de 14.02.2019.

1. Gus W. Weiss, The Farewell Dossier, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm , accesat în data de 14.02.2019.
2. Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, Edit. The Langner Group, Arlington | Hamburg | Munic, 2013, p.3.

serviciilor destabilizate. Așa numitul *„război cibernetic"* a devenit în prezent o parte oarecum intrinsecă a conflictelor internaționale. Cu atât mai mult cu cât, datorită naturii sale nedetectabile și a potențialului de a provoca daune fizice fără a detașa forțe militare umane sau mecanizate, devine de departe o metodă preferată de atac, tot mai des întâlnită.

Fără a face o analiză asupra *„cifrei negre"* a atacurilor[1] asupra infrastructurilor critice ale oricărui stat, pot afirma că există o nevoie crescândă de specialiști de securitate cibernetică pentru identificarea și gestionarea nu doar a breșelor de securitate, ci și a atacurilor de tip persistent sau ascuns.

Atacurile cibernetice pot constitui o amenințare chiar la adresa suveranității statelor Uniunii Europene, aici putem aminti cazul Estoniei, din 2007, când întregul sistem de comunicații electronice a fost paralizat pentru 22 de zile prin atacuri de tipul „negare de servicii" sau, generic denumit, atac de tip DDoS. În timpul atacului din Estonia, serviciile bancare au fost inactive, operatorii de telefonie au rămas fără serviciu de acoperire, mass-media online și paginile oficiale ale guvernului au fost compromise sau închise[2].

Pentru a arăta amploarea fenomenului și posibila dimensiune a unui atac cibernetic, putem evidenția atacul WannaCry, care a fost activat în 99 de țări cu un număr de peste 75.000 atacuri într-o singură zi, toate luând forma unui atac cibernetic de răscumpărare, afectând serios instituții vitale ale statelor din lumea întreagă, precum Serviciul Național de Sănătate (NHS) din U.K, unde au fost infectate un număr de 16 instituții medicale, unele companii de comunicații din Spania, printre care firma de telecomunicații Telefonica, compania de gaze naturale, compania electrică Iberdrola și câteva instituții de

1. *Cifra neagră a atacurilor în acest context simbolizează numărul real al atacurilor ca sumă a atacurilor declarate adunate cu cele nedeclarate sau neindetificate.*
2. Andreas Schmidt, „The Estonian Cyberattacks", în *The fierce domain –conflicts in cyberspace 1986-2012* (ed. Jason Healy), Edit. Atlantic Council, Washington, D.C, 2013, p. 9.

învățământ din Italia. Per ansamblu, așa-numitul atac de răscumpărare „WannaCry" a afectat zeci de mii de computere, inclusiv în România, SUA, Marea Britanie, China, Rusia sau Taiwan.

Experții în domeniul securității IT spun că atacurile au fost legate și fost numit cel mai mare atac de răscumpărare din istorie. Hackerii au cerut bani pentru a returna informațiile furate. Potrivit securlist.com[1] și Kaspersky Lab, România se situează în partea de sus a țărilor cele mai afectate de malițiosul „WannaCry", situându-se în clasament imediat după Rusia, Ucraina, India, Taiwan, Tadjikistan, Kazahstan, Luxemburg și China.

Agențiile de știri străine au raportat că atacul a afectat, de asemenea, cele peste 1.000 de sisteme informatice ale Ministerului de Interne din Rusia, precum și Deutsche Bahn, care este una dintre cele mai mari companii de transport din Germania.

Pentru a justifica și fundamenta eventuale propuneri de dezvoltare a unor standarde și politici de securitate cibernetică relevante și comune la nivel european, trebuie să reidentificăm, dintr-o perspectivă statistic calitativă, contextul de securitate cibernetic actual. Așadar, în urma analizei datelor raportate[2] și menționate în conținutul lucrării, se observă o creștere a numărului de publicări cu privire la încălcările normelor și legilor naționale, respectiv internaționale, la scară largă. Acest lucru sugerează că o dată cu creșterea numărului de încălcări ale principiilor securității în sectorul cibernetic crește și impactul asupra statelor și a organizațiilor generatoare de securitate.

După cum afirmam, vom aduce mai aproape numerele care vor decide traseul insecurității cibernetice, desigur, dintr-o poziție

1. GReAT, *„WannaCry ransomware used in widespread attacks all over the world"*, 12.05.2017 https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/, accesat în data de 15.02.2019.
2. Varonis, „Data Under Attack: 2018 Global Data Risk Report from The Varonis Data Lab", https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf, accesat în data de 23.04.2019.

empirică. Așadar, în perioada 1 ianuarie 2005 - 18 aprilie 2018, s-a înregistrat un număr de 8.854 brețe de securitate doar în SUA[1].

În contextul de securitate din sectorului privat, cifrele date de brețele de securitate la nivel global nu arată deloc bine.

Deoarece cercetarea de față este elaborată într-o perioadă de 4 ani, doresc să evidențiez în mod exclusiv cazuistica cea mai relevantă la nivel global, cu influențe în zona UE pentru perioada 2016-2018.

Drept urmare, în cursul anului 2016, gigantul Yahoo - care este parte din Oath, o companie a Verizon - a anunțat că un număr de aproximativ 3 miliarde de conturi de email Yahoo! au fost sparte, remarcându-se faptul că aceasta a fost una dintre brețele de securitate semnificative pentru utilizatorii online ai statelor membre UE și, în același timp, pentru multe dintre organizațiile care foloseau serviciile de corespondență electronică ale acestui furnizor, având o anvergură economică și de scurgere de date extraordinară, probabil printre cele mai mari de până acum din istoria internetului[2]. În același an (2016), Uber a raportat pe site-ul oficiat că hackerii au furat datele cu caracter personal - nume, prenume, e-mail, numărul de telefon șamd. - ale peste 57 de milioane de utilizatori ai sistemului Uber și ale șoferilor înregistrați în acel moment în sistem.[3]

Cu toate că aplicația nu este atât de populară nici în România și nici în Europa, se cuvine totuși amintit următorul caz. În 2017, atât aplicația cât și site-urile Friendfinder au fost sparte, iar în urma acestor atacuri un număr de ~412 milioane de conturi de utilizatori au fost accesate. Drept urmare, s-a angajat o companie specializată în

1. Centrul de Resurse pentru Furtul de Identitate, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf, accesat în data de 23.04.2019.
2. Yahoo! Help, „Yahoo 2013 Account Security Update FAQs”, https://help.yahoo.com/kb/account/SLN28451.html?impressions=true, accesat în data de 23.04.2019.
3. Dara Khosrowshahi, Uber Newsroom, „2016 Data Security Incident”, https://www.uber.com/newsroom/2016-data-incident/, accesat în data de 23.04.2019.

securitate cibernetică pentru a investiga breșa, dar raportul acesteia nu a fost făcut public.[1]

După cum s-a mai amintit, un număr de peste 100.000 de grupuri din cel puțin 150 de țări și un număr de ~417.000 terminale au fost infectate de virusul WannaCry în cursul anului 2017, acest lucru având un impact financiar de aproximativ 4 miliarde de dolari - aici nefiind incluse cele peste 600.000 terminale care au accesat benevol IP-ul de pe care se desfășura atacul.

Atacurile orientate spre terminalele care minează monezi digitale (*criptomonedă*) - *care implică acțiuni de tipul criptojacking* - au crescut cu 8500% în 2017 față de 2016, iar în același interval de timp 5,4 miliarde de atacuri ale virusului WannaCry au fost blocate.[2]

În acest context, în cursul anului 2017, s-a blocat un număr de ~8.684.000 de aplicații mobile, adică un număr de 23.800 de aplicații mobile rău intenționate blocate în fiecare zi.[3]

În 2019, doar 24% dintre alertele organizațiilor care au experimentat atacuri cibernetice asupra infrastructurii tehnologice operaționale s-au dovedit a fi reale, acestea fiind în scădere față de anul 2018, când procentul acestora a atins 34%[4].

În martie 2018, Under Armor a raportat că datele a 150 de milioane de utilizatori ai aplicației „My Fitness Pal" au fost compromise[5].

---

1. Steve Ragan, SCO, „Researcher says Adult Friend Finder vulnerable to file inclusion vulnerabilities", 2016, https://www.csoonline.com/article/3132533/researcher-says-adult-friend-finder-vulnerable-to-file-inclusion-vulnerabilities.html, accesat în data de 23.04.2019.
2. Symantec, *Internet Security Threat Report*, Vol.23 p.5, http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_, accesat în data de 23.04.2019.
3. *Ibidem*, p.80.
4. CISCO, Benchmark Study, „Anticipating the Unknowns", https://ebooks.cisco.com/story/anticipating-unknowns#!/page/1, accesat în data de 23.04.2019.
5. Under the Armor, Press Release, „Under Armour Notifies MyFitnessPal Users Of Data Security Issue", http://investor.underarmour.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue?ReleaseID=1062368, accesat în data de 23.04.2019.

Chiar și în prezent, deși a fost mediatizată problema, angajații sectorului militar utilizează echipamente și aplicații care au capacitatea nu doar de geolocalizare, dar și de utilizare de la distanță ori interceptate pentru a li se urmări activitatea deținătorilor și a celor cu care interacționează. Nu este un caz singular și nu este vorba doar despre personalul militar român, american șamd. Unul dintre cazurile cele mai sensibile este dat de deconspirarea unor baze militare secrete, a traseelor urmate de personalul acestora și de identitate lor[1], iar un alt caz asemănător, dar cu date nu atât de sensibile, ar fi cel al bazei militare de la Deveselu, unde este instalat scutul antirachetă al SUA[2]. Acestea sunt numai câteva exemple reprezentative ale faptelor comise în acest mediu virtual. De semnalat este faptul că atacurile cibernetice de tipul „*ransomware*" sunt cel mai des întâlnite în țările în care utilizarea internetului este mai mult decât o obișnuință, acolo unde aceasta este chiar o necesitate. Putem urmări noile abordări ale administrațiilor locale sau guvernamentale de implementare a soluțiilor „orașelor inteligente", unde aproape totul este interconectat și aproape interdependent, totul este online.

Undeva la 60% din totalul domeniilor malițioase sunt asociate cu campanii de tip „*spam*".

În urma acestor atacuri, s-a identificat faptul că infectarea cu aplicații malițioase și atacurile de tipul „*web-based*" sunt, din perspectiva apărării cibernetice, printre cele mai costisitoare, marile organizații fiind obligate de contextul de insecuritate să facă o infuzie de aproximativ 2.4 milioane $.

1. Liz Sly, „U.S. soldiers are revealing sensitive and dangerous information by jogging", 29.01.2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?noredirect=on&utm_term=.c3748d111f92, accesat în data de 03.05.2019.
2. Harta Interactivă STRAVA, Baza Militară de la Deveselu, Jud. Olt, 03.05.2019, https://www.strava.com/heatmap#14.04/24.38239/44.07120/hot/all, accesat în data de 03.05.2019.

Într-un procent de aproximativ 38%, cele mai utilizate formate de documente în transportul aplicațiilor malițioase sunt cele generate de suita Microsoft Office (Word, Power Point și Excel), pe când aplicațiile corelate cu viața de zi cu zi a persoanelor (Audio, Video, Streaming, Monitorizare a sănătății șamd.) au cel mai ridicat grad de infestare cu elemente malițioase.

În ceea ce privește scurgerea de informații din telefoanele mobile inteligente, această breșă este dată în mod deosebit de utilizarea unor aplicații care oferă această oportunitate. Drept urmare, datele culese de pe echipamentele de comunicații inteligente sunt într-o proporție de 63% numere de telefoane mobile și de 37% locații ale dispozitivelor. Odată cu aceste meta-date[1] sunt culese adrese de email date bancare, utilizatori și parole. Se prognozează că până în 2020 numărul total de parole utilizate de sistemele automate și utilizatori va ajunge la ~300 miliarde.

Un număr de aproximativ 21 dintre documentele existente pe terminalele informatice nu sunt protejate de măsuri specifice de securitate, iar organizațiile, în general (41%), au un număr mediu de ~1000 documente sensibile neprotejate în sistemele informaționale proprii. Asta în condițiile în care undeva la 70% din organizații consideră că securitatea datelor gestionate este suficient dezvoltată, deși riscurile și posibilitățile unui atac cibernetic au crescut considerabil. Realitatea este că, în anul 2017, un procent de 61% au fost organizații cu până în 1000 de angajați.

Prognozele arată că atacurile cibernetice asupra industriei medicale se vor multiplica cu 400%, iar organizațiile în general vor cădea

1. Aleksandar Kovačević, Dragan Ivanović, Branko Milosavljević, Zora Konjović, Dušan Surla, „Program electronic library and information systems”, în *Automatic extraction of metadata from scientific publications for CRIS systems*, Vol. 45, Nr. 4, p. 377, https://www.researchgate.net/profile/Dragan_Ivanovic/publication/216592386_Automatic_extraction_of_metadata_from_scientific_publications_for_CRIS_systems/links/0fcfd50cb052fcdf77000000/Automatic-extraction-of-metadata-from-scientific-publications-for-CRIS-systems, accesat în data de 03.05.2019.

victime ale atacurilor cibernetice de tip „*ransomware*" cu ritm de o organizație la fiecare 14 secunde. Costurile acestor tipuri de atacuri, estimate în anul 2019, sunt de ~11.5 miliarde $.

Tot în 2017 variantele de aplicații malițioase apărute pe piață au crescut cu 54% și imediat corelat cu aceasta s-au identificat creșteri ale procentelor de raportare a vulnerabilităților echipamentelor de comunicații fixe și portabile cu 13% față de anul 2016, iar creșterile în sectorul infrastructurilor critice sunt de 29%.

Ce ne transmit toate aceste date enumerate mai sus? Deși datele expuse sunt în cea mai mare parte culese din organizațiile sectorului privat, acest lucru nu înseamnă că statul și instituțiile statului sunt lipsite de aceste riscuri, vulnerabilități, ori sunt ferite de atacuri. Mesajul este foarte clar direcționat asupra fiecărei forme de guvernământ a lumii. Atacurile cibernetice se înmulțesc într-un mod exploziv, amenințările și riscurile par să fie tot mai mari, vulnerabilitățile sunt tot mai multe, iar atacurile tot mai complexe și cu efecte tot mai dezastruoase.

Impactul pe care acest sector, parțial controlat, îl are asupra suveranității statelor este unul destul de serios. Fie că vorbim despre conceptul realismului ori ideologia supranaționalismului un lucru este cert, suveranitatea statului și a spațiului virtual în raport cu securitatea națională este vitală.

Nesiguranța, lipsa capacității de apărare, răspuns ori recuperare în urma unor astfel de campanii de atac duc în primă etapă la dizolvarea principiilor și formei organizației direct implicate, iar mai apoi la vulnerabilizarea siguranței și securității naționale.

Una dintre cele mai urgente măsuri pentru a contracara acest tip de atac pe viitor este, potrivit analiștilor de securitate și a analiștilor din sectorul relațiilor internaționale, o legislație pe măsura pericolului, iminent de altfel[1].

1. Alina Grigoraș Butu, "WannaCry ransomware attack: Romania the 9th most affected country, securelist.com says. Dacia Mioveni plant's IT system failed", 13.05.2017,

În contextul de securitate a Uniunii Europene, apare în 2013 un nou element de noutate. Politica cibernetică a UE, pentru a asigura un grad de reziliență echidistant, real și egal la nivelul statelor membre, aduce în prim plan necesitatea de armonizare a legislației orientate pe securitate și reziliență cibernetică. Ca urmare a acestor tumultoase interese comune, Comisia Europeană emite *Comunicare Comună* către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, *„Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat"*.[1]

Uniunea Europeană, drept urmare, se obligă să asigure și să întărească eforturile țărilor membre în această materie și în demersul de a oferi cetățenilor proprii acces la resursele internetului la scară largă, condiționat de asigurarea integrității și securității spațiului virtual și de perspectiva, respectiv atitudinea mai ofensivă și rezilientă la actele malițioase sau criminale în sectorul cibernetic.

Pentru ca acest obiectiv să poată fi realizabil este nevoie de o capacitare și o extindere a UE în vederea conlucrării cu sectorul privat pentru o aplicare conformă și reală a Strategiei. Așadar, securitatea cibernetică transcende dincolo de colaborarea internațională interguvernamentală, redefinind poziția UE în contextul de securitate comună al statelor membre.

III.2.3. Guvernare supranațională elitistă asupra sectorului de securitate cibernetic

Emblematic, acest subcapitol poate primi titlul *„Între Guvernarea Elitelor și Guvernanța Elitelor în Sectorul Cibernetic"*.

https://www.romaniajournal.ro/wannacry-ransomware-attack-romania-the-9th-most-affected-country-securelist-com-says-dacia-mioveni-plants-it-system-failed/, accesat în data de 15.02.2019;

1. Comisia Europeană, „Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat", https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:RO:PDF, accesat în data de 22.04.2019.

Sunt două aspecte care necesită lămurire. Primul aspect se referă la nevoia de a înțelege ce înseamnă o elită, care sunt acestea și unde le găsim sau formăm, iar cel de-al doilea aspect se referă strict la modalitatea de guvernare a acestor elite în sectoarele de activitate în care sunt mobilizate.

Adesea se confundă guvernanța unei elite cu modul în care aceasta este guvernată într-un sistem de guvernământ, ceea ce mă face dator în a veni cu o explicație pragmatică asupra acestui fapt. Totodată, consider mai mult decât necesară analiza conceptului de elită definit de o funcție, precum cea de decident sau conceptul definit de capacitatea personală a celor puțini în fața majorității.

În era globalizării, pe lângă dilema suveranității federațiilor raportată la suveranitatea statelor membre, întâlnim o reală confuzie cu privire la actul de guvernare în raport cu ceea ce trebuie guvernat. Oricum ar fi, un lucru este cert, abordarea marilor puteri este un rezultat al exercițiilor îndelungate, un rezultat al reușitelor și al eșecurilor, drept urmare este abordarea cea corectă și demnă de urmat, altfel spus, calitatea și resursele statului primează indiferent de miză - în sistemul globalizării, statul este pe primul loc, necondiționat, acesta contează mai mult, nu mai puțin decât orice altceva[1].

III.2.4. Teoria elitelor și decidentul în actul de guvernare a spațiului cibernetic

Pornind de la cunoașterea argumentelor și teoriilor celor trei fondatori ai școlii elitiste italiene, Vilfredo Pareto (1848-1923), Gaetano Mosca (1858-1941) și Robert Michels (1876-1936), înțelegem și care sunt influențele acestora asupra politologilor și a teoriilor elitismului contemporan sub a căror indirectă guvernare ne regăsim.

Desigur, în contextul științelor politice ori sociologie, teoria elitelor este orientată înspre actul de guvernanță al statului care încearcă

1. Thomas L. Friedman, *op.cit.*, p.153.

să definească, să descrie și să explice relațiile de putere în societatea contemporană. Rezumând, teoria susține că o mică minoritate, alcătuită din membri ai rețelelor de elită economică și de planificare a politicilor, deține cea mai mare putere, iar această putere este independentă de alegerile democratice. Cu toate că sunt date definiții mai ample, esența lor este aceeași. Fie că modalitatea de alegere a unei elite este dată de corporații, administrații sau de influența rețelelor de specialitate, membrii „elitei" - elitiștii - exercită în permanență o putere semnificativă asupra deciziilor corporative și guvernamentale, asupra sectoarelor public și privat în context național, european și internațional cu extindere la nivel global. Nu fac referire aici la analize cu obiectiv primar, identificarea celor mai înstăriți oameni ai lumii, este un snobism declarat, referirea se face în contextul nevoii unei guvernanțe elitiste a noului areal cibernetic, care într-un mod natural trebuie guvernat. Un aspect comun cu clasicele teorii ale elitelor este dat de caracteristicile fundamentale ale teoriei care evidențiază că puterea este concentrată, elitele sunt unite, non-elitele sunt diverse și pasive chiar non-reactive, interesele elitelor sunt unificate, datorate unor cauze, medii și poziții comune, iar caracteristica definitorie a puterii este poziția organizațională. Grupurile de apartenență arbitrare, precum nobilimea, rasa, sexul sau religia sunt, evident, complet excluse din rețelele tradiționale de putere ale statului și apar în opoziție grupuri izolate, motivate de ideologii segregaționiste. Teoria elitelor se opune pluralismului, iar, în cazul Uniunii Europene, este evidentă respingerea tradițiilor sau cutumelor care presupun că toți indivizii, sau cel puțin multitudinea de grupuri sociale, au puteri egale și echilibrează reciproc balanța decizională, contribuind la rezultatele politice democratice, care reprezintă voința agregată și emergentă a societății. Teoria elitelor susține fie că democrația este o utopie, așa cum se vede în contextul de guvernare italian conservator, fie că democrația nu este realizabilă în capitalism.

Îmbrățișând elitismul lui Floyd Hunter (1912-1992), bazat pe promovarea celor care se remarcă prin calități deosebite, extraordinara capacitate de conducere și guvernare a resurselor pentru obținerea unui rezultat ideal, consider că elitismul stă la baza unei bune guvernanțe a spațiului cibernetic și doar cu o bună gestionare a acestor resurse se poate proiecta un spațiu virtual comun, mai sigur și mai eficient.

Elita cibernetică este reprezentată atât de capacitățile de necontestat și de dorit ale persoanelor active în mediile profesionale în diversitatea lor, cât și de funcția potrivită acesteia, cu rol consultativ ori de decizie într-o problematică de securitate a informației. Necesitatea acestui concept, elitismul, în arealul de guvernare al sectorului informațional, este nu doar o nevoie reală, cât o obligativitate a statelor de a-și împlini nevoile și obiectivul primordial de protejare a suveranității teritoriale din punct de vedere jurisdicțional, geografic și virtual. Decidenții, în toate nuanțele lor, precum cei politici, financiari și de ce nu, decidenții autodeclarați, recunoscuți sau anonimi, dar care au un cert impact în zona de formare a opiniei publice, pot lua cea mai înaltă formă decizională în ceea ce privește elitismul societal în raport cu impactul pe care îl au asupra societății și factorilor de decizie naționali (*n.r. liderii organizațiilor non guvernamentale, asociațiilor civile, asociațiilor profesionale sau comunităților religioase*).

III.2.5. Actorul de securitate

Abordarea securității din perspectiva actului discursiv ridică întrebări cu privire la relația dintre actori și analiști în procesul de definire și înțelegere a agendei de securitate, în condițiile în care actorul de securitate iese din definiția elitelor sectorului de securitate, acesta primind o definiție mai largă.

Într-un spectru general, aprecierea securității obiective este dincolo de mijloacele noastre de analiză. Principala idee este că actorii

și publicul lor securizează anumite probleme într-o anumită formă a actului de securitate. Actorii care securizează nu rostesc neapărat cuvântul „securitate” și nici utilizarea de către ei a termenului securitate nu constituie neapărat un act de securizare[1] .

La nivel aproape global, cu precădere în mediul politic, se observă o lipsă acută de experiență și informație la nivel de decizie politică de securitate. Putem lua ca studiu de caz aproape fiecare minister în parte, unde personaje cu o educație, formare și experiență în orice alt domeniu decât cel al securității mediului pe care ar trebui să îl guverneze iau adesea decizii de o implicație majoră fără a se consulta cu analiștii, experții sau practicienii din acest domeniu specific. Aproape de fiecare dată la scurt timp apar repercusiunile (dezastruoase uneori) care nu întotdeauna sunt soluționate prin luarea deciziei corecte sau cel puțin anularea celei greșite.

Fundamentând cu nevoile stringente ale populației și entităților publice ori private față de ceea ce noi numim securitate, doresc să evidențiez nevoia de pregătire de specialitate în fiecare sector în parte a fiecărui actor și de flexibilitate a acestuia în a fi perfectibil pentru a ajunge la nivelul de elită în mediul pe care îl guvernează sau pe care îl va guverna.

Așadar, rezumându-ne la domeniul securității cibernetice, putem identifica mai multe arii care necesită o atenție sporită față de ceea ce înseamnă o guvernare elitistă.

III.2.6. Organigrama sectoarelor securității cibernetice din spațiului cibernetic

Pentru a putea identifica nevoia de guvernare a unei federații, a unei țări sau a unei organizații, este necesară cunoașterea părților componente ale acestora. Conștientizând acest aspect, suntem nevoiți

1. Barry Buzan, Ole Wæver, Jaap de Wilde, *Securitatea. Un nou cadru de analiză*, Edit. CA Publishing, Cluj-Napoca, 2011, pp.56- 57.

să audităm sau să chestionăm acest sector și să generăm un raport cât mai fidel realității, în baza unei analize de detaliu pe toate ariile unde mediul virtual este prezent, are implicații majore, sau poate fi influențat. Voi descrie o hartă relațională a domeniului cibernetic din perspectiva nevoii de a-l guverna cât mai eficient, prin identificarea nu doar a pilonilor principali care compun domeniul securității cibernetice, ci și a nevoilor privind resursa umană și a cunoștințelor necesare.

Noțiunea și esența securității cibernetice nu poate fi disjunsă de contextul guvernanței spațiului cibernetic. Guvernanța spațiului cibernetic, respectiv guvernanța securității spațiului cibernetic, în contextul studiul dilemei de securitate cibernetică, sunt determinante pentru dezvoltarea durabilă a acestuia. Cu alte cuvinte, cele două concepte sunt necesare pentru preîntâmpinarea inițierii sau escaladării dilemei de securitate cibernetică.

Reglementarea spațiului cibernetic în spațiul internațional și implicit în spațiul național și aplicarea legii nu pot fi nicidecum neglijate, de vreme ce spațiul cibernetic este un areal activ (virtual) comun de securitate, libertate și prosperitate economică. Posibilitatea unei soluții de implementat pentru soluționarea pașnică a dilemei de securitate cibernetică și evitarea coliziunii dintre nevoia de supra-securizare, *„și pentru a obține mai multe drepturi și libertăți în spațiul cibernetic ar fi ca securitatea, libertatea și prosperitatea economică în mediul virtual să fie universal recunoscute drept drepturi fundamentale ale utilizatorilor în egală măsură. De principiu, optimul de guvernanță în spațiul cibernetic va fi atins atunci când va exista o analogie ușor identificabilă între nivelul de securitate, libertate și prosperitate din spațiul cibernetic*"[1].

Domeniul guvernanței securității spațiului cibernetic este susținut de nouă piloni principali:

1. Iulian Popa, *Securitatea și guvernanța spațiului cibernetic contemporan* (teză de doctorat), Universitatea Babeș-Bolyai, Cluj-Napoca, 2015, pp.133-134.

- Arhitectura de Securitate;
- Operațiuni de Securitate;
- Guvernanța Cibernetică;
- Managementul Riscului;
- Educația de Securitate;
- Pregătire profesională continuă;
- Intelligence de Securitate;
- Norme și Standarde;
- Securitate Fizică.

În acest context, în baza unui studiu lansat în 2017[1], am adoptat și dezvoltat organigrama domeniului de securitate cibernetică, conform ***Anexei nr.3,*** intitulată *„Organigrama Domeniilor Guvernanței Securității Cibernetice”*. Desigur, această organigramă reprezintă evidențierea principalelor domenii ale practicii de securitate cibernetică și a interdependențelor dintre acestea. Securitatea cibernetică nu se rezumă la activitatea de „hacking”. Într-o anume măsură, cuprinde și conceptul de hacking, dar este mult mai mult de atât.

Practic, guvernanța securității cibernetice și guvernanța spațiului cibernetic sunt două arii de cercetare diferite. În acest studiu se pune un accent deosebit pe guvernanța securității cibernetice. În condițiile în care limba engleză este neoficial utilizată la scară largă atât în limbajele de programare, cât și în context filosofic cu referire la conceptele securității cibernetice, pentru a nu cădea în derizoriu, atât în conținutul lucrării, cât și în construirea hărții relaționale a guvernanței securității cibernetice, am utilizat terminologia din limba engleză și o adaptare prin viziunea proprie a acestor termene la terminologia din limba română.

Obiectivul a fost atins în momentul în care am identificat, pe lângă zona de practică a activității de Securitate a informației, o

1. Henry Jiang, „The Map of Cybersecurity Domains (version 1.0)”, 10.02.2017, https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/, accesat în data de 03.05.2019.

arie prea puțin cunoscută de majoritatea practicienilor, guvernanța domeniilor securității cibernetice.

Deși, într-o oarecare măsură, majoritatea domeniilor și punctelor exemplificate în această hartă sunt interconectate și dependente de întreg, doresc să aduc în atenție un domeniu elocvent lucrării de față, cel al Guvernanței Securității Cibernetice (*Cyber Security Governance*).

Considerăm că avem un cadru conceptual, împreună cu o metodologie practică pe care o organizație o folosește pentru a-și defini și implementa strategia de abordare a amenințărilor contradictorii legate de dependența sa de spațiul cibernetic. În special, acest cadru le permite organizațiilor să își articuleze strategiile pentru abordarea amenințării persistente avansate (APT) sau pentru abordarea unor atacuri cibernetice directe de tip DDoS, ransomware șamd. Acest cadru reprezentat în organigramă definește patru niveluri de pregătire organizațională, caracterizate prin:

- Perspectiva organizației;
- Posibile amenințări cibernetice;
- Strategia organizației de abordare a amenințărilor survenite asupra sistemului informațional al organizației, incluzând aici și analiza tactică, tehnică și procedurală adoptate de atacator;
- Poziția adoptată de organizație în raport cu guvernanța securității cibernetice.

Rezumându-ne la guvernanța securității cibernetice, putem spune că această se desfășoară în patru planuri, anume:

- *Legi și Regulamente;*
- *Proceduri de Control Organizațional;*
- *Audit;*
- *Implicarea Managementului Executiv.*

Primul plan este cel la care orice organizație trebuie să se alinieze, indiferent de aria de activitate, sectorul de apartenență (politic, militar, civil, privat, public șamd.), volumul de informații gestionat ori chiar țara de proveniență.

În acest prim plan *conformarea* se face contextual pe trei nivele:

- *Statal sau național* - referindu-ne strict la alinierea organizației la legislația națională, la regulamentele organismelor guvernamentale și publice, dar nu în ultimul rând la cutumele naționale în materie fără a încălca legislația națională și internațională;
- *Federal/Unional* - Uniunea European, prin construcție fiind o federație de state membre cu scopuri, obiective și viziune comună într-o lumină supranațională, emite cadrul legislativ internațional la care țările membre sunt obligate să se alinieze. Desigur, conformarea organizațiilor la acest nivel se face și în raport cu tratatele dintre UE, statele membre și spațiul non-UE, în contextul economic, politic sau militar;
- *Specific Industriei* - Deoarece industria tehnologiei informației și a comunicației este mai vastă decât pare, pe parcursul dezvoltării acesteia la nivel global, au apărut, pe lângă Cadrul de referință și Standardele naționale ori internaționale, înțelegeri (uneori nescrise sau oficializate) privind utilizarea, construcția, funcționarea ori compatibilitatea elementelor componente din industria IT&C.

Cel de-al doilea plan este orientat spre *conceperea și implementarea procedurilor de control organizațional* prin:

- *Politici* - generate sau emise în urma analizării Cadrului de referință și a Standardelor naționale ori internaționale aplicabile în organizație și aliniate la cadrul legislativ corespunzător;
- *Proceduri* - emise cu scopul de a crea un sistem rezilient, segmentat și cu o capacitate de recuperare optimizată în baza resurselor organizației;
- *Ghiduri* - reprezentate de nevoia de oferi un timp răspuns minim, aproape instant, la cazuri izolate precum evenimentele ori incidente de securitate;

- *Conformare și Implementare* - Reprezintă obiectivul principal al unității de control de securitate. Orice proces activ sau pasiv din componența sistemului de securitate al unei organizații este obligatoriu a fi în conformitate și implementat conform cadrului normativ actualizat din aria de acțiune din care face parte.

Al treilea plan este *Auditul*, care, desigur, poate fi de două tipuri, intern sau extern. Importanța auditului este dată de impactul financiar generat de rezultatul acestuia în raport cu viabilitatea, redundanța și reziliența sistemului de securitate al organizației.

Ultimul plan este orientat pe implicarea managementului executiv în buna guvernanță a sectorului cibernetic din organizația pe care o administrează. Acest lucru, de cele mai multe ori, din cauza lipsei unei viziuni tehnice de detaliu a conducerii organizației, se recomandă a fi realizat prin aplicarea unui sistem de management informatic centralizat, cu capacități de generare de rapoarte și statistici în timp real. Aici mai adăugăm încă două instrumente care pot fi folosite:

- Indicatorii de performanță (KPI), care utilizează măsurătorile specifice organizației pentru a înțelege cât de bine îndeplinesc angajații, unitățile de afaceri, proiectele și subunitățile obiectivele strategice;
- Indicatorii de risc (KRI) așa cum sugerează și numele măsoară riscul. Instrumentele KRI sunt folosite de organizații pentru a determina cât de mult sunt acestea expuse riscului sau cât de riscant este un anumit proiect sau activitate. KRI-urile reprezintă o modalitate de a cuantifica și monitoriza cele mai mari riscuri la care este expusă o organizație (sau o activitate). Prin măsurarea riscurilor și a impactului lor potențial asupra performanței acestora, organizațiile pot crea sisteme de avertizare timpurii, care să le permită să monitorizeze, să gestioneze și să atenueze riscurile iminente.

În același plan mai avem *Informarea Riscului*, care încorporează o evaluare a semnificației de siguranță sau de risc relativ. Această abordare asigură că sarcina de reglementare impusă de un cadru normativ sau de un proces este adecvată importanței sale în protejarea sănătății și siguranței publice și a mediului, dar și a datelor în raport cu acestea. Importanța cea mai mare o dă rezultatul unei decizii bazate pe o informare completă a riscului în organizație.

Ținând cont de cercetarea explorativă a guvernanței domeniilor securității cibernetice, putem observa că există o oportunitatea de dezvoltare a acestui domeniu din punct de vedere strategic și operațional pentru îmbunătățirea oricărui sistem de securitate organizațional.

Concluzii preliminare

Guvernanța spațiului virtual, fie că este analizată în conceptul realismului sau studiată în lumina supranaționalismului, trebuie înțeleasă și abordată având la bază principiul respectării echilibrului de forțe și a suveranității statelor și a formelor de organizare supranaționale.

Noutatea apare în urma abordării unui spațiu care nu este reglementat și normat suficient, precum este spațiul terestru de exemplu. Abordarea nu poate fi decât una explorativă, deoarece încă sunt multe domenii de cercetare care își abandonează resursele fizice limitate și migrează spre acest nou areal virtual numit *„spațiul cibernetic”*, ale cărui limite sunt date de nevoile noastre de dezvoltare.

Pentru a putea scoate în prim plan tranziția de la spațiul real la cel virtual, este nevoie să cunoaștem cel puțin impactul pozitiv și negativ adus de acesta de la apariție până în prezent. Urmând cursul scurtei și tumultoasei istorii a ciberneticii, realizăm că este un domeniu care necesită o atenție chiar mai sporită decât spațiul cotidian, fizic. Motivul este lesne de înțeles, s-a constatat în urma analizelor din ultimii zeci de ani că progresul este exploziv și deja impactul cuantificat în

resurse informaționale, economice, sociale, politice și militare este uriaș. În acest context, se poate face o comparație conform căreia noul mediu cibernetic este unul care poate fi comparabil cu saltul de la candelă la electricitate.

Odată cunoscute aceste două medii, după cum menționam, printr-o cercetare explorativă, putem să ne lansăm în încercarea de a reformula, readapta sau anula anumite teorii și concepte care până acum au funcționat.

Realismul politic este o teorie care încearcă să explice relațiile internaționale în termeni de putere. Realismul politic presupune că oamenii sunt egoiști prin natură, cei mai importanți actori din politica internațională sunt state, mediul internațional este unul de anarhie în care statele se află în conflict constant între ele în căutarea interesului rațional propriu, iar moralitatea nu numai că nu este importantă, dar poate fi contraproductivă pentru obiectivul supraviețuitor. De vreme ce statele diferă în capacitatea lor de putere, adesea vor forma alianțe pentru a crea un echilibru de putere cu scopul de a preveni instabilitatea politică și războiul.

Neorealismul, cunoscut și ca realism structural, se concentrează mai degrabă pe structura sistemului internațional decât pe caracteristicile individuale de putere ale fiecărui stat. Neorealismul consideră că sistemul internațional poate fi descris în termeni de polaritate sau de centre de putere. Un sistem multipolar este unul în care statele acționează relativ independent unul față de celălalt. Un sistem bipolar constă din două centre de putere, iar statele gravitează în jurul unuia dintre ele. Într-un sistem unipolar există o mare putere, un hegemon, care poate influența toate celelalte state.

Realismul politic are atât puncte forte, cât și puncte slabe. Este adesea un punct de plecare semnificativ în analiza cauzei conflictului în relațiile internaționale și poate oferi o perspectivă asupra modului de prevenire a conflictului larg prin intermediul, de exemplu, a echilibrului puterii. Cu toate acestea, acesta oferă o imagine incom-

pletă a unui sistem internațional complex și a forțelor din interiorul acestui mecanism.

Aspectele de noutate în cazul acestui studiu privind guvernanța spațiului virtual în lumina analizei conceptelor realism și supranaționalism sunt date de implicațiile progresului exploziv al industriei tehnologiei informației și a comunicațiilor. Dezvoltarea și inovarea în acest domeniu a adus experții în științele politice, sociale sau de securitate la un punct în care sunt nevoiți să schimbe, fundamental chiar, teorii și considerații bazate pe premise care nu conțineau sub o formă sau alta conceptele sectorului cibernetic, a mediilor virtuale, digitalizarea și echipamentele electronice. Se ridică noi întrebări de cercetare, care pun experții într-o situație stânjenitoare, aceștia trebuind să răspundă la întrebări privind granițele spațiului cibernetic, normarea, legiferarea, jurisdicția și suveranitatea statelor ori a federațiilor asupra spațiilor în care acest nou areal cibernetic se desfășoară și asupra standardizării, normării și reglementării în ceea ce privește utilizarea acestuia și de către cine.

În actual context geopolitic și de securitate în care România deține calitatea de stat membru al UE, pot afirma că progresul UE în lumina supranaționalismului dă roade vizibile, iar țările membre se aliniază într-un mod natural. Organismele supranaționale ale UE se bucură de o atenție sporită din partea statelor membre, iar în ultimul an se discută tot mai des de apariția unei armate a UE, care să fie compusă din resursele militare ale statelor din întreaga uniune. În acest context, consider oportună o readaptare a teoriei elitelor și a decidentului de securitate în actul de guvernare a spațiului cibernetic, orientată spre progres tehnologic, cercetare, inovare și dezvoltare a sistemelor de securitate.

Capitolul IV.
Diplomația în spațiului cibernetic

VI.1. *„România Digitală"* o nouă perspectivă

Odată cu cunoașterea glosarului de termeni diplomatici, a protocolului diplomatic și a aplicabilității noțiunilor de diplomație tradițională în noua formă de diplomație, care parcă este fundamentată într-o cu totul altă știință decât cea a relațiilor internaționale și negocierilor, se poate observa cum ia naștere din diplomația tradițională o nouă formă a diplomației, anume diplomația modernă, aproape post-modernă aș putea zice. Aceasta, prin adoptarea conceptelor fundamentale ale diplomației clasice și adaptarea acestora la epoca contemporană (digitalizată) se metamorfozează, aducând în prim plan o triadă diplomatică formată din diplomația tradițională, „diplomația digitală" și „diplomația cibernetică".

Deoarece adesea se face o confuzie între „e-diplomație", „diplomația digitală" și „diplomația cibernetică" și mai mult decât atât, se

face o confuzie în relația dintre diplomație și spațiul digital/virtual, consider de bun augur să ofer o explicație pragmatică.

Urmărind dezbaterile, interviurile și declarațiile de presă ale înalților demnitari români, observăm că există o tendință a acestora de a folosi uneltele și mijloacele existente în sectorul cibernetic/virtual, cu scopul de a evidenția, trata și expune o oarecare activitate diplomatică sau de a duce situațiile de caz în această zonă. Dintre aceste mijloace pot aminti rețelele de socializare, paginile de internet specializate sau alte mijloace de expunere în mediul virtual. În același timp, trebuie să recunoaștem că luăm parte la un fenomen de digitalizare a diplomației, prin utilizarea întregului arsenal digital pus la dispoziție omului modern și accesul la vastul ocean informațional din mediul virtual, precum a extraordinarei dezvoltări tehnologice, acestea două fiind adesea într-o simbioză aproape perfectă și într-o relație de interdependență absolută. Uneltele care sunt aduse în soluționarea situațiilor diplomatice (*problemelor, incidentelor, conflictelor șamd.*) în sectorul cibernetic nu mai sunt cele utilizate acum 30 de ani. Există un interes deosebit din partea Guvernului României și a ministerelor de resort în a-și asigura confidențialitatea, integritatea, disponibilitatea și autenticitatea datelor și informațiilor vehiculate, acum mai mult decât de obicei datorită preluării Președinției Consiliul Europei de către România. Cum este și normal, sunt suplimentate eforturile și în planul protecției și securizării informației vehiculate în mediile fizice și electronice, odată cu intensificarea participării reprezentanților ministerelor la activități internaționale, organizate în cadrul structurilor europene. De asemenea, se recomandă ca în detrimentul transportării informațiilor „la purtător" să se utilizeze cele consacrate și/sau utilizarea terminalelor sistemului EXTRANET.RO - sau similar, pentru transmiterea, respectiv pentru primirea informațiilor clasificate.

Din această perspectivă, consider relevantă menționarea unuia dintre multele instrumente digitale, utilizat la randament maxim,

care a întors soarta alegerilor prezidențiale în 2014, anume Facebook. Succint, strategia utilizată de echipa de campanie online a domnului președinte Klaus Werner Iohannis în timpul alegerilor pentru funcția de președinte al României în 2014 a fost bazată, în principal, pe crearea de imagine și marcă (branding) online, apoi pe strategia de conținut și diseminare activă. A fost o campanie alimentată în mod deosebit cu materiale de promovare text, video, foto, grafică și încercări cu succes de încurajare a inițiativelor de tip „*grass-roots*". Trebuie evidențiat în acest caz specific că datorită terenului câștigat în prima campanie din 2014 și a menținerii aceleiași strategii de imagine pe parcursul mandatului, pentru alegerile prezidențiale din 10.11.2019 și 24.11.2019 nu a mai fost necesară o astfel de campanie de mobilizare, drept urmare Klaus Werner Iohannis a rămas președintele României în exercițiu.

Analiza perspectivei demografice evidențiază concentrarea pe mobilizarea potențialei mase de oameni pentru participarea la vot - între 18-35 de ani în mediul urban, ceea ce reprezintă cu aproximație populația activă pe Facebook în perioada campaniei. Au fost utilizate metodologii de cercetare bazate pe chestionare și sondaje asociative, testare A/B, soluții de „*data-warehouse*".

La apogeul activității s-a identificat un număr de 200.000 de oameni, la circa 100.000 de fani. Așadar, conform raportului emis de echipa tehnică care s-a ocupat de această promovare, în total s-a ajuns la 400.000 de fani și un număr de fani secundari de 600.000 care interacționau permanent cu informările (postările) sau materialele difuzate exclusiv prin intermediul canalului de socializare Facebook. Asta în condițiile în care s-a difuzat cam jumătate din suma de resurse emisă de grupurile de campanie ale doamnei Macovei, Udrea sau a domnului Ponta. S-a utilizat mai mult ca niciodată transmisia în direct prin Facebook, care a mobilizat o mare masă de oameni la vot.[1]

1. Crişan Andreescu, „Klaus Iohannis, Facebook. Cine este omul din spatele președintelui ales care i-a adus peste un milion de fani", 20 nov 2014, https://www.dcnews.ro/

Pe de altă parte, același mediu virtual, cu aceleași instrumente, se poate întoarce împotriva echipelor de promovare ale partidelor din lumea întreagă și împotriva dorinței politicului de a atinge obiectivul scontat. Exemplific aici cazul depistat chiar de Facebook în luna februarie 2019, unde printr-un interviu telefonic, Nathaniel Gleicher, șeful departamentului de securitate cibernetică al Facebook a comunicat pentru Ziarul Adevărul faptul că s-a eliminat un număr de 31 de pagini, grupuri și conturi Facebook din România, care erau parte a unei rețele coordonate *„menite să inducă oamenii în eroare, ai căror utilizatori „operează în România pentru a promova o narațiune pozitivă în legătură cu PSD”. La analiza condusă de Facebook și-au adus aportul raportările venite din surse deschise de informații și probele aduse din partea partenerilor Facebook activi ca și actori non statali în sectorul de securitate cibernetică*. În ciuda eforturilor de conspirare a persoanei din spatele acestei operațiuni ample, s-a identificat atât persoana cât și întreaga topologie a rețelei de dezinformare, cunoscută ca fiind o campanie de tipul *„fake news*”. S-a constatat că în acces direct cu aceste postări eronate au intrat un număr de 1.500 de urmăritori (followers) și a fost implicat un bugetul de publicitate pentru perioada 2013-februarie 2019, relativ mic, de 650 de dolari americani[1]. Această întreagă operațiune de deconspirare a unui mecanism, vădit malițios, cu intenția clară de dezinformare, a adus un deserviciu nu doar partidului de guvernământ din România în 2019, ci și tuturor reprezentanților acestui partid în organismele internaționale. Este un deserviciu diplomatic adus României în an centenar și mai ales în perioada în care țara deține președinția UE.

Așadar, putem observa cum instrumente moderne, precum rețelele de socializare și orice alt canal de comunicare activ pot fi nu doar

klaus-iohannis-facebook-cine-este-omul-din-spatele-pre-edintelui-ales-care-i-a-adus-peste-un-milion-de-fani_460018.html, accesat în data de 14.07.2018.

1. Denis Grigorescu, „Cum a depistat Facebook ‚laboratorul de troll al PSD”, în *Adevărul*, 12.03.2019, p.3.

„o altă unealtă” ce poate fi utilizată în vederea atingerii obiectivelor diplomatice, ci chiar mijlocul în sine de obținere a rezultatului dorit. Exemplul de mai sus nu face altceva decât să sublinieze importanța instrumentelor diplomației digitale.

Desigur, beneficiile utilizări acestor instrumente sunt vaste, dar totodată utilizarea incoerentă și iresponsabilă a acestora poate aduce mari deservicii parcursului actului/procesului diplomatic. Contextual, găsim actori statali care consideră că afirmarea unor opinii proprii prin diverse canale de comunicare online este total inofensivă. Utilizarea unui astfel de instrument, într-un mod iresponsabil și lipsit de diplomație, având o certă calitate de reprezentant al statului (președinți, prim miniștri, consuli șamd.) nu face altceva decât să degenereze un conflict, să creeze un eveniment sau incident de securitate, sau în cel mai bun caz să ridice semne de întrebare la adresa instituției și guvernării statului din care face parte. Dintre nenumăratele exemple, pot aduce în atenție utilizarea echipamentelor mobile inteligente în timpul întâlnirilor cu un grad ridicat de importanță și unde conținutul discuțiilor purtate poate aduce atingeri grave relațiilor internaționale sau integrității instituțiilor și verticalității unor persoane. Când menționez utilizarea acestor echipamente mobile inteligente, mă refer la înregistrarea foto - audio - video din timpul întâlnirilor și transmiterea acestor informații în spațiul public prin intermediul rețelelor de socializare și nu numai. În urma unui asemenea incident, rezultatele de la masa negocierilor (*și nu în cazuri izolate*) au fost revizuite și desigur schimbate.

Rolul diplomației cibernetice și a diplomației digitale în buna guvernanță a informației din spațiul cibernetic poate fi cu adevărat înțeles printr-un studiu inductiv și introspect a relației și evoluției fenomenului de tranziție de la diplomația tradițională la cea modernă.

IV.2. Diplomația digitală și Diplomația cibernetică

Diplomația digitală, în contextul Diplomației Publice, ne aduce în prim plan noi perspective, realiste desigur, de practicare a diplomației cu ajutorul instrumentarului cibernetic, astfel încât aproape că putem vorbi de o schimbare de paradigmă. Odată cu utilizarea noului instrumentar diplomatic, actul diplomatic, cândva identificat a fi o activitate exclusivistă, clasificată și protejată corespunzător, a devenit un act public în cea mai mare parte, elitelor cerându-li-se să devină mult mai flexibile în ceea ce privește munca diplomatică, ajungându-se până la a se permite ca munca depusă în timpul actului diplomatic să fie vizibilă publicului larg.[1]

Cu toate că la nivel internațional cercetătorii și practicienii din sectorul științelor diplomației încearcă să găsească noi mijloace de facilitare a actului diplomatic, în ceea ce privește sectorul cibernetic, majoritatea rezultatelor din teorie și practică au fost încercări de obținere de rezultate prin rețele sociale și interfețe ale acestor rețele. Scopul primar a fost de a transmite informația diplomaților, guvernelor sau formatorilor de opinie într-un mod cât mai eficient, într-un timp cât mai scurt, cu implicarea minimului de resurse, la un nivel de impact cât mai ridicat.[2]. Unele țări au mers până la a-și instrui ambasadorii să aibă un blog sau chiar să stabilească un număr minim de „tweeturi” pe săptămână. Utilizarea în sistemul diplomatic a riscurilor de social media a ajuns până acolo încât acestea au ajuns la forma unui verb neregulat, precum: blogurile ambasadorilor, primul ministru a postat pe pagina sa de Facebook, prim secretarul de stat a postat un mesaj pe Twitter. Utilizarea non-strategică a rețelelor sociale poate distrage atenția diplomaților de la alte activități mai importante.

---

1. Corneliu Bjola, „Digital diplomacy - the state of the art”, în *Global Affairs*, Vol.2, Nr. 3, Edit. Routledge Taylor & Francis Group, 2016, pp.297-298.
2. Shaun Riordan, *The Strategic Use of Digital and Public Diplomacy in Pursuit of National Objectives*, Edit. Top Open Printing Sytems S.L., Barcelona, 2016, p.10.

Utilizarea eficientă a mediilor sociale solicită timp și resurse. Timpul petrecut în menținerea conturilor Instagram, Twitter sau Facebook este rupt din timpul necesar întâlnirilor cu contactele față în față, care sunt încă esențiale pentru construirea rețelelor diplomatice. Nu contează dacă mijloacele de comunicare socială reprezintă un mijloc eficient de asigurare a obiectivelor diplomatului și sunt desfășurate în mod deliberat în acest scop. Este mult mai grav dacă oportunitățile diplomatice și informațiile geopolitice esențiale sunt pierdute doar pentru a asigura prezența pe Web 2.0. Diplomații ar trebui să ia în considerare, de asemenea, dacă conținutul postărilor lor într-adevăr atinge interesele țării lor sau promovează reputația lor într-un mod care le sporește șansele de a-și realiza misiunea. Oricum ar fi analizat, în cele din urmă, accentul obsesiv asupra diplomației digitale în rețelele de socializare online distrage atenția de la gama mult mai largă de instrumente digitale disponibile pentru actorii guvernamentali și neguvernamentali în mediul internațional, trivializând însăși valoarea socială a rețelelor de socializare online.[1]

Consider mai mult decât potrivită aducerea în prim plan a ceea ce înseamnă, definitoriu chiar, diplomația digitală, care, în opinia mea, reprezintă actul de utilizare a tuturor instrumentelor digitale și ale tehnicilor diplomatice (*incluzând aici și diplomația consulară*), Diplomația cibernetică, este definită de utilizarea întregului instrumentar diplomatic (*strategia diplomatică, resursele umane, resursele materiale, resursele informaționale*) în vederea soluționării situațiilor care necesită o atenție sporită, apărute în sectorul cibernetic sau virtual.

Diplomația digitală în România este reprezentată prin utilizarea de către instituțiile de stat specializate, ambasade, consulate și chiar de către diplomați a paginilor sau portalurilor web instituționale, a căsuțelor de poștă electronică, a rețelelor de socializare (Facebook, Twitter, YouTube șamd.), precum și a instrumentelor puse la dispoziție, precum echipamente electronice fizice și programe informatice

1. *Ibidem.*

(aplicații online / offline, baze de date, echipamente de criptare, echipamente de comunicații audio-video șamd.).

Un aspect important este legat de rețelele sociale ce se dezvoltă la nivelul fiecărui utilizator cu o calitate oficială. Acestea pot să ajungă să își piardă relevanța. Motivul este unul simplu; nu toți urmăritorii canalului sau profilului prin care se transmite informația sunt și susținători ai celui care este identificat cu acest canal sau profil. Cu alte cuvinte, comunitatea formată prin aceste metode nu este neapărat cea mai eficientă în promovarea resurselor, datelor și informațiilor transmise prin aceste canale de comunicare.

Presa modernă, prezentă adesea prin diferite forme de jurnale sau ziare digitale, este concentrată mai mult ca niciodată pe numărul de clicuri și accesări ale paginilor sale, pe care, la rândul ei, le folosește pentru a promova diverse forme de publicitate. Compartimentele mass-media sociale din mediul online au fost înființate pentru a activa, fără intenție, în detrimentul calității jurnalistice. Relațiile și contactele cu corespondenții străini de lungă durată, de carieră chiar, cu competențe lingvistice relevante și cunoștințe istorice, au fost de multe ori tăiate. Rezultatul este că presa digitală se luptă să facă bani, în timp ce substanța informațiilor transmise prin intermediul acesteia a scăzut în ciuda efortului de a asigura numărul de accesări sau clicuri propus. Bazându-se în mod esențial pe aceleași surse de informație, presa postmodernă a ajuns să producă materiale mai mult sau mai puțin relevante și să renunțe la o formă și conținut bazate pe calitate, analiză și sinteză a informațiilor culese. Tragic este că rezultatul presei digitale a ajuns aproape o nonvaloare pentru beneficiari, această informație nemaifiind corelată la o valoare pe care aceștia să fie dispuși să o plătească. Informarea a luat forma unui „tweet" cu o aprobare superficială printr-un „like" sau în cel mai bun caz un comentariu, care adesea se dovedește a fi subiectiv.

Există pericole similare pentru guvernele sub-naționale și pentru actorii societății civile.

Criteriul nu ar trebui să fie cuantificat în numărul de membri ori urmăritori, legături sau prieteni existenți pe canalele de comunicare online sau rețelele de socializare din mediul virtual, ci mai degrabă în existența unui număr restrâns de oameni relevanți (cu influență în domeniul de specialitate) în virtutea scopului pentru care aceste informații au fot diseminate și care să fie direct interesați de esența materialelor obținute prin aceste canale de comunicare. Dacă instrumentele digitale sunt văzute doar ca instrumente, atunci ele pot fi integrate cu succes într-o strategie diplomatică mai amplă. Dar mai întâi trebuie concepute obiectivele și o strategie. Dacă actorii diplomatici din cadrul organismelor internaționale și naționale, fie din cadrul guvernelor subnaționale sau chiar actorii societății civile, stabilesc obiective clare - să înțeleagă ce încearcă să realizeze - atunci pot alege între o gamă largă de instrumente diplomatice, inclusiv instrumente publice și digitale, pentru a selecta combinația corectă pentru a asigura cele mai bune obiective. Strategiile reușite sunt probabil hibride, în măsura în care combină instrumentele digitale cu cele non-digitale. Cu toate că instrumentele digitale sunt cele mai rapide și eficiente mijloace de comunicare, cu un important rol ca factori de multiplicare a informației, acestea nu sunt neapărat cea mai bună soluție în generarea conținutului care trebuie comunicat sau diseminat pentru a fundamenta o posibilă influență asupra celor din comunitate.

Guvernele învață că pot influența relațiile internaționale într-un mod pozitiv numai dacă au ceva care contribuie la rezolvarea problemelor internaționale (după cum s-a menționat în lucrare, branding-ul național - echivalentul marketingului pentru guverne). Același lucru rămâne valabil și pentru guvernele subnaționale și pentru actorii societății civile. Instrumentele digitale funcționează cel mai bine ca instrumente de replicare și multiplicare a informației pentru obținerea unei influențe, acestea nu sunt creatoare de influență. După cum am sugerat mai sus, o mare parte din discuțiile și practica diplomației

digitale s-a axat pe rețelele sociale online. În această ordine de idei, s-a analizat și s-a constatat existența unui mod de adaptare a diplomației la instrumentele moderne de socializare deja existente, fie Twitter, Facebook, LinkedIn sau, într-o mai mică măsură, Instagram. Protecția consulară, o parte centrală a diplomației pentru guverne (deși poate mai puțin pentru actorii societății civile), s-a concentrat pe utilizarea mijloacelor de informare socială digitală pentru a alerta cetățenii în situații de criză și pentru a identifica unde pot exista cetățenii aflați în dificultate.

Sistemul „*RO-ALERT*”, care este funcțional, fiind „*implementat pe teritoriul României de către Ministerul Afacerilor Interne, prin Inspectoratul General pentru Situații de Urgență și cu suportul tehnic al Serviciului de Telecomunicații Speciale, ca urmare a Ordonanței de urgență nr. 72 din 5 octombrie 2017*”[1], funcționează prin comunicarea unor mesaje de alertă abonaților de pe teritoriul României prin intermediul operatorilor de servicii de comunicații mobile, pe echipamentul mobil, dar cu mențiunea că există o nevoie de compatibilitate între sistemul de comunicații și unele echipamente care nu se încadrează cerințelor minime solicitate de funcționalitatea sistemului „RO-ALERT”. În unele state europene există sisteme asemănătoare, dar care comunică - transmit - mesaje SMS. Aceste alertări sunt transmise în funcție de contextul și natura stării de urgență identificate la nivel regional - fenomene meteorologice cu înalt grad de risc, incendii majore din zonele populate, riscul de explozie și alte calamități ori situații de risc pentru populația dintr-o anumită regiune. Mediatizarea acestui proiect, pentru a putea atinge un nivel ridicat de conștientizare a populației, a fost efectuată în paralel cu implementarea sistemului de alertare, ocazie cu care a fost desfășurată și o campanie de informare publică, conștientizare și pregătire a populației pentru utilizarea sistemului „RO-ALERT”.[2]

1. Sistemul „*RO-ALERT*”, https://ro-alert.ro/, accesat în data de 27.11.2019.
2. Comunicat ANCOM: „Sistem Alert de avertizare în cazuri de urgenţă”, http://www.ancom.org.ro/sistem-alert-de-avertizare-in-cazuri-de-urgenta-_5811, accesat în data

În ceea ce privește instrumentarul tehnologic utilizat de diplomați în ziua de azi, consider necesară conceperea unui sistem unic, modular și dinamic, care să poată fi adaptat la portofoliul și profilul fiecărei persoane care activează în sectorul diplomatic și la contextul în care acesta activează. Un astfel de sistem ar putea fi parte din fluxul informațional închis și deschis, intern și extern, cu capacitatea de a avea integrate toate rețelele de socializare online, canalele de comunicare audio, video, text și chiar instrumentele de analiză, monitorizare și alertare, care însumate formează un sistem de tip „*Big Data*[1]"

IV.2.1. Tehnologia „*Big Data*" și Diplomația digitală

În ceea ce privește utilizarea tehnologiilor „Big Data" în sectorul diplomației, se pot aduce argumente solide în favoarea implementării de sisteme bazate pe această nișă a culegerii și prelucrării datelor din sectorul cibernetic și a valorificării informațiilor în scopul îndeplinirii actului diplomatic.

Tehnologiile Big Data permit colectarea unor cantități mari de date din toate echipamentele conectate la o sursă de internet și utilizate de către o persoană sau un sistem automat. Aceste tehnologii sunt utilizate în prezent în mare măsură pentru cercetarea pieței, dar trebuie recunoscut nu doar potențialul, ci și aplicabilitatea acestei tehnologii în sectorul guvernamental. Algoritmii sunt în curs de dezvoltare, dar cu toate că analiza datelor nu a ajuns încă la maturitate, aceasta permite, de exemplu, agențiilor de publicitate să vizeze publicitatea personalizată și introdusă sub nasul utilizatorului terminalelor inteligente după o profilare specifică intereselor utilizatorului, obținută pe baza datelor extrase de pe aceste terminale.

Recunoscând oportunitatea, mulți diplomați au început să abordeze soluțiile oferite de tehnologia „Big Data". Oportunitatea utili-

---

de16.08.2018.

1. Barbara, Diplo, „Big data: The next accelerator for diplomacy?", https://www.diplomacy.edu/blog/big-data-next-accelerator-diplomacy, accesat în data de 16.08.2018.

zării datelor la nivel diplomatic este recunoscută în zilele noastre de toate statele, datele și informațiile înlocuiesc fără de tăgadă țițeiul, așa cum descoperirea valorii acestuia a înlocuit aurul la un moment dat în istorie. Cea mai valoroasă resursă a lumii nu mai este țițeiul, ci sunt datele[1].

În primul rând, datele influențează mediul în care funcționează diplomații. Digitalizarea a dus la reconceptualizarea valorilor materiale și desigur a monedei, drept urmare fluxul de date conturează modalitatea de gestionare a banilor în general. Geopolitica și Geoeconomia bazate pe date sunt influențate de apariția unor noi reguli cu noi seturi de date, acestea sunt fundamental reformate.

În al doilea rând, datele introduc noi subiecte, noi provocări și elemente strategice la masa negocierilor și elaborării politicilor, începând cu protejarea vieții private și a datelor personale, până la economia digitală și comerț.

În al treilea rând, datele și informațiile oferă diplomaților instrumente noi pentru a face față provocărilor sectorului geopolitic contemporan și aduc activitățile diplomatice la un grad mult mai eficient. Două dintre cele mai importante tehnologii utilizate în acest caz sunt „data mining" și inteligența artificială[2].

IV.2.2. Tehnologii de comunicare și monitorizare

Sunt dezvoltați algoritmi asemănători care identifică mai multe date decât s-ar putea colecta la o simplă întâlnire cu utilizatorii acestor echipamente, indiferent dacă aceștia sunt doar turiști, emigranți temporari pe piața muncii sau rezidenți în străinătate. Acești algoritmi identifică numeroase date, precum limba vorbită (chiar și ambiental,

1. The Economist, Leaders, „The world's most valuable resource is no longer oil, but data - The data economy demands a new approach to antitrust rules", 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, accesat în data de 24.04.2019.
2. Barbara, Diplo, „Big data: The next accelerator for diplomacy?", https://www.diplomacy.edu/blog/big-data-next-accelerator-diplomacy, accesat în data de 24.04.2019.

fără ca telefonul să se regăsească într-o convorbire), date privind localizarea geografică, temperatura, umiditatea, pulsul, itinerarul zilnic parcurs, altitudinea la care se găsește, numărul de echipamente cu care este interconectat, locațiile unde au fost făcute plățile cu ajutorul telefonului, agenda telefonică și în general datele întregului sistem de operare (incluzând aplicațiile mobile) cu care telefonul este dotat, accesul la microfon și cameră etc. În cazul unei crize consulare într-o anumită țară, ministerele de externe ar putea să vizeze și să lanseze mesaje personalizate către cetățenii lor, despre care au informații că ar putea fi acolo. Citirea mesajelor de către persoana vizată ar spune ministerului de externe exact unde se găsește cu exactitate fiecare proprietar de terminal digital care a primit acest mesaj, permițând planificarea de eventuale misiuni de salvare. Ceea ce este considerat un subiect controversat este faptul că ministerul de externe ar putea să activeze de la distanță dispozitivul de localizare GPS din aceste terminale pentru a determina unde este, chiar dacă nu a fost pornit (ceea ce ar putea fi util dacă proprietarul acestuia a fost mort sau rănit). Astfel de abordări sunt controversate din cauza posibilității utilizării acestor instrumente de către serviciile de informații și de organizațiile criminale pentru supraveghere, atât legale, cât și ilegale a persoanelor. Acestea ridică probleme majore privind confidențialitatea. Dar tehnologii similare sunt deja întâlnite pe piața internațională sau sunt dezvoltate în scopuri de marketing și publicitate, mai ales în scop de profilare. Ar fi necesare mici modificări ale acestora și cu ușurință ar putea fi adaptare instrumentarului ministerelor de externe, care le-ar putea utiliza pentru îmbunătățirea serviciilor consulare și de strângere de informații și nu numai.

Instrumentele diplomației digitale sunt eficiente atunci când sunt alese, proiectate, dezvoltate și aplicate în vederea atingerii unor obiective clare, fie de către guverne, guverne subnaționale sau actori ai societății civile. Într-adevăr, este mai important ca actorii societății civile, cu resursele lor mai limitate, umane, financiare și cele privind

reputația adesea scăzută, să cunoască și să înțeleagă ce anume doresc să obțină cu ajutorul acestor instrumente și platforme în spectrul diplomației digitale și să aibă cu criterii clare de cuantificare.

În acest subcapitol, principalele „activități diplomatice" vor fi împărțite în trei categorii:

A. Diplomația digitală în contextul Diplomației publice: modelarea mediului politic și social internațional;
B. Construirea de rețele;
C. Culegerea de informații și managementul cunoașterii;

Datorită faptului că aceste instrumente și platforme digitale existente sunt produse preponderent informatice, pot fi dezvoltate și bineînțeles aplicabile în mai multe sectoare ale diplomației moderne.

IV.2.3. Instrumentarul diplomatic digital

În măsura în care noile abordări ale diplomației publice s-au concentrat asupra utilizării zonei social media existente, în acest capitol este tratată interacțiunea diplomației publice și digitale, subliniind în special faptul că prezența în activitățile diplomatice cu ajutorul Web 2.0 nu înseamnă neapărat doar influență, ci poate submina eficiența altor activități, care contextual pot fi mai eficiente în soluționarea diferitelor situații. Există însă și alte aspecte care ar trebui avute în vedere. Rețelele de socializare online pot fi instrumente foarte imprevizibile și fără un rezultat cert și scontat. Lansarea unui mesaj prin intermediul acestor rețele poate deveni viral sau poate fi pierdut fără a avea impactul scontat. Comentatorii se concentrează pe exemple în care campaniile online au avut succes. În această ordine de idei, trebuie să fim conștienți că, spre deosebire de informația în format fizic, informația în format digital ridică un anumit grad de risc în ceea ce privește accesarea, copierea/multiplicarea, alterarea sau ștergerea de la distanță - interceptarea acesteia este unul dintre

obiectivele primordiale ale unui atac cibernetic -[1]. Astfel, prin intermediul arealului cibernetic informația se poate răspândi cu o viteză mult mai mare decât prin mijloacele tradiționale de corespondență și cu această scalabilitate a vitezei crește și posibilitatea dezinformării. Astfel, Facebook și Twitter au avut un rol cheie în fenomenul primăverii arabe.

Cu toate acestea, avem tendința să ignorăm numeroasele campanii sau mesaje lansate pe rețelele de socializare online care au dispărut fără urmă. În cartea sa din anul 2007, *„Lebăda neagră”*[2], Nassim Taleb face o pledoarie plăcută de a-și aminti cimitirele ca istorie, pe măsură ce el se opune erorii narative. În aceeași ordine de idei, suntem cu toții îndrumați să ne amintim, să cercetăm și să investigăm cimitirele digitale pentru resursele ce zac neatinse și neexplorate în ele sau, în ceea ce privește prezentul capitol, pentru nenumăratele campanii care nu au devenit virale în comparație cu cele ce au devenit virale. Consider că suntem obligați să înțelegem diferențele dintre medii (real sau virtual) și să identificăm lucrurile comune care se regăsesc în aceste medii pentru a oferi cel mai bun rezultat. În fapt, realizăm faptul că dacă o anumită campanie devine sau nu virală nu are nimic de-a face cu calitatea sau importanța mesajului sau cu competențele digitale ale celor care lansează campania. Am fi îndreptățiți să afirmăm că acest fenomen de obținere a viralului are mult mai mult de a face cu norocul și contingența. De aceea trebuie să fim conștienți de faptul că niciodată nu este bine să ne bazăm rezultatele și reușita pe utilizarea unui singur instrument, o singură metodă sau tehnică. Strategia trebuie să fie una bogată compusă dintr-un instrumentar bogat. Prin urmare, dependența de sectorul mass-media online și uti-

1. Ioana Vasiu, Lucian Vasiu, *Informatică Juridică și Drept Informatic*, Editura Albastră, Cluj-Napoca, 2009, p.153.
2. Nassim Nicholas Taleb, *Lebăda neagră - Impactul foarte puțin probabilului*, Edit. Curtea Veche, București, 2008.

litatea rețelelor de socializare online pentru a lansa campanii tematice - în special pentru actorii societății civile - are un grad ridicat de risc.

Dacă guvernele, la nivel național, subnațional sau la nivelul grupărilor și asocierilor societății civile, doresc promovarea unui proiect sau a unei campanii specifice cu sprijinul instrumentarului de socializare online, acestea pot maximiza șansele de a avea un impact prin pregătirea în primul rând a terenului. Acest lucru are mai multe implicații. În primul rând, este important să fie identificate resursele necesare pentru atingerea obiectivelor. Acestea pot fi persoane sau instituții, dar este necesar să găsiți modalități de a le activa în strategia aleasă și de a vă asigura că aceștia citesc conținutul promovat. Ca în cazul diplomației publice non-digitale, conținutul contează. Este necesară construirea și stabilirea unei reputații pe termen lung; lucrurile interesante și relevante pot avea șansele scontate în a fi percepute conform planificării dacă și numai dacă persoanele care citesc mesajul acorda credit și atenție campaniei lansate. În al doilea rând, trebuie să se stabilească credibilitatea pe termen lung. În al treilea rând, campaniile hibride, care combină instrumente online și offline, au o probabilitate crescută de succes. După cum veți observa mai jos, crearea rețelelor virtuale funcționează cel mai bine atunci când sunt întărite de contactele personale; relațiile interumane și socializarea interpersonală stau încă la baza oricărei rețele, fie acestea chiar și virtuală. Organizarea unui atelier de lucru și apoi promovarea concluziilor sale prin rețele și canale de comunicare socială în mediul virtual și prin diverse medii sociale, sau prin utilizarea unui atelier pentru a aduce formatorii de opinie față în față și factorii de decizie care au avut o certă activitate în mediul online pot fi abordări eficiente ale campaniilor hibride. În cele din urmă, diferitele platforme media sociale virtuale/digitale au caractere și caracteristici diferite. Asemenea ziarelor din trecut, ceea se poate face pe o singură platformă și modul în care se face acest lucru pe acea platformă nu este neapărat aplicabil pe o altă platformă. Beneficiarii serviciilor de promovare de

conținut prin rețelele de socializare online sunt foarte conștienți de acest lucru. Cu siguranță, nimeni nu va posta pe LinkedIn imagini și păreri de la petrecerea avută cu o seară în urmă, precum nici nu veți regăsi postări legate de locul de muncă pe Facebook, pe când Twitter este folosit în principal pe dispozitive mobile, iar utilizatorul are nevoie de o gândire mai clară și mai rapidă și exprimare de substanță într-un număr limitat de cuvinte. Cei care utilizează mediile sociale ca instrument în sectorul diplomației publice trebuie să identifice raportul dintre utilizatorii acestora și conținutul emis pe acestea, echilibrul lingvistic, lipsa de ambiguitate și cea mai bună formulare a conținutului pentru a crea un factor de impact cât mai ridicat.

După cum am arătat și mai sus, rețelele de socializare online nu sunt singurele instrumente digitale pe care guvernele și grupurile societății civile le pot folosi pentru a modela mediile de politică. O atenție sporită este acordată educației pentru utilizarea jocurilor, în special a jocurilor pe calculator, ca instrumente educaționale. În parte, aceasta urmărește să profite de entuziasmul generațiilor întregi de a juca jocuri pe calculator - *dacă joacă oricum jocurile, de ce nu le facem educative?* De asemenea, jocurile pe calculator pot fi mult mai eficiente decât predarea tradițională în promovarea cursanților autodidacți, care sunt capabili să se adapteze flexibil la mediile în schimbare rapidă. Dar dacă acest fenomen poate fi folosit pentru a educa, atunci înseamnă că poate fi folosit și pentru a modela mediul politic și social, ca ecosistem. În loc să folosească mediile virtuale, unde acest conținut să fie promovat pe diverse canale de comunicare digitală, actorii diplomatici pot crea jocuri care să îi încurajeze pe jucători să se gândească la anumite probleme sau să experimenteze anumite medii în moduri care pot să le modeleze gândirea cu privire la lucrurile care sunt o vulnerabilitate, un risc sau o simplă situație corijabilă în societatea din care aceștia fac parte.

Prin intermediul simulatoarelor animate și a jocurilor de simulare, beneficiarii observă dintr-o altă perspectivă ceea ce poate au

cunoscut la un nivel superficial prin modul în care designerul jocului a modelat simularea. Exemple la nivel european sunt mai multe. Banca Centrală Europeană (BCE) a elaborat un joc (€CONOMIA - The Monetary Policy Game)[1] pentru a preda elevilor de liceu politica monetară. Jocul, €CONOMIA, oferă jucătorilor o varietate de date economice și apoi îi invită să stabilească ratele dobânzilor băncilor centrale. Jucătorii obțin scorul în funcție de modul în care rezultate lor sunt în conformitate cu ținta de inflație a BCE (aproape, dar sub 2%). Deși jocul pretinde a fi pur educativ, el modelează în mod inevitabil felul în care jucătorii se gândesc la politica economică și monetară europeană, în special modul în care problemele sunt încadrate și limba în care sunt discutate. Jocul nu garantează faptul că jucătorii vor fi prezenți la propunerile de politici specifice ale BCE (și BCE ar pretinde că nu este ideea jocului), dar face aceast lucru probabil.

Există o hibridizare a educației prin elemente tradiționale cu și prin intermediul instrumentelor digitale, fenomen care trebuie susținut, dar trebuie și dezvoltat, fiind deosebit de important atât în educație, cât și în alte forme de formare (autorul explorează dezvoltarea jocurilor online pentru formarea diplomaților și directorilor de afaceri în analizarea și gestionarea riscului geopolitic). Există o reală probabilitate ca aceste metode moderne de dezvoltare a gândirii și viziunii prin aplicații informatice și jocuri informatice / simulatoare să poată oferi un real ajutor în simularea de scenarii privind strategiile aplicate în diplomație în general.

IV.2.4. Rețelele diplomatice - interdependența real/virtual

Trebuie recunoscută valoarea rețelelor de socializare online în crearea și extinderea rețelelor diplomatice, întrucât în trecut rețelele trebuiau să fie construite în mare parte prin relaționarea interpersonală, metodă care era limitată de bariere geografice. Acum putem vorbi

1. €CONOMIA – The Monetary Policy Game, http://www.ecb.europa.eu/ecb/educational/educational-games/economia/html/index.en.html, accesat în data de 21.08.2018

despre rețele globale, care pot fi susținute activ prin intermediul platformelor rețelelor de socializare online. În timp ce Facebook tinde să fie folosit pentru rețele personale, LinkedIn este folosit mai mult pentru rețele profesionale și pentru promovarea serviciilor. În ceea ce privește eficiența, calitatea este mai importantă decât cantitatea. Este ușor să obții 20.000 de adepți pe Twitter, dar inutil dacă nu citesc mesajele comunicate. Construcția rețelei devine astfel strategică pe baza obiectivelor stabilite pentru strategia diplomatică, iar apoi contextual, devine un instrument de atingere a obiectivelor, o rețea cu caracter operațional.

Strategia diplomatică stabilește tipul de contacte pe care ar trebui să se concentreze rețeaua, precum și rolul acestor adepți / parteneri din rețea. Rețelele servesc atât pentru strângerea de informații, cât și pentru transmiterea și multiplicarea influenței în rândul maselor, a comunităților sau doar la nivel de individ. Utilizarea resurselor obținute prin intermediul rețelelor virtuale nu poate duce la atingerea scopurilor diplomatice (fie că vorbim despre diplomația publică sau cea consulară) prin ele însele fără a utiliza și alte unelte din instrumentarul diplomatic. Eficiența poate fi observată conform Figurii nr.5, aceasta fiind dată de implicațiile diplomației cibernetice în raport cu diplomația consulară / publică, combinând instrumentele online cu contactul personal / relațiile interpersonale.

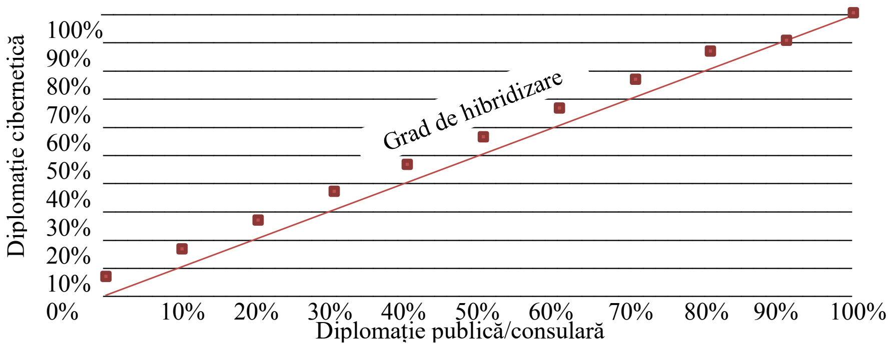


Figura nr.19. Grafic privid rezultatele aduse de Diplomația cibernetică în raport cu Diplomația publică / consulară

Acest lucru poate funcționa în ambele sensuri. Rețelele construite inițial prin intermediul rețelelor sociale pot fi consolidate prin contact mai personal, fie prin trimiterea de mesaje personale, fie prin contact fizic în timpul vizitelor sau invitațiilor la conferințe sau alte evenimente. De asemenea, relațiile inițial stabilite prin contactul fizic la conferințe sau alte evenimente pot fi consolidate și menținute prin intermediul rețelelor sociale și al altor platforme digitale. Social media poate facilita, de asemenea, construirea rețelei indirecte cu acele contacte care ar putea să nu vrea să aibă contact direct cu dvs., fie din cauza unui dezacord politic, fie pentru că ar provoca stânjenire în cercul lor social sau politic. Deși o abordare hibridă, care combină construcția relațiilor online și offline, este, în general, cea mai bună abordare a construirii rețelelor, uneori absența contactului offline poate fi un avantaj.

Putem considera, dintr-un punct de vedere primitiv, că pe baza uneltelor diplomației digitale se pot crea conexiuni cu factori decizionali, formatori de opinie, specialiști șamd. în vederea obținerii unui contact personal, față în față, ceea ce de cele mai multe ori duce la o creare, întărire sau extindere a rețelelor internaționale. Chiar și diplomații guvernamentali dezvoltă rețele de contacte în țara în care activează și le întrețin chiar și după retragerea acestora din respectivele țări, mai mult, le lasă „moștenire" celor ce-i precedă. În general, acestea devin rețele mamut, care solicită un anumit grad de organizare și o segmentare clară, întemeiată pe o bază relațională care să deservească diplomatul în obținerea cu ușurință a contactelor în cel mai scurt posibil pentru împlinirea actului diplomatic. Trebuie menționat faptul că o astfel de rețea, actuală și funcțională, se poate răspândi pe o arie geografică mare, pe mai multe nivele și categorii, astfel de rețele necesită ani pentru a fi construite și secunde pentru a fi destructurate. În ceea ce privește comunicarea, conținutul este esențial. Conținutul trebuie să aibă o anumită formă, să fie construit și adaptat, nici mai mult nici mai puțin, la motivului din spatele

conținutului livrat. Acesta trebuie să ajute la construirea credibilității și motivației în construirea rețelelor, precum și la menținerea unei reputații crescute. Tranzacționare informaților și a ideilor a avut un rol esențial în construirea rețelei diplomatice în era pre-digitală și rămâne astfel valabilă și de actualitate și în era contemporană. În cele din urmă, tehnicile online și offline se completează într-o armonie perfectă, care duce la o creșterea progresivă a rețelei. Mediile sociale din sectorul cibernetic se dezvoltă și duc la o expansiune a rețelelor. Oricât de performante ar fi, rețelele existente și utilizate în mediul virtual nu oferă conținutul sau profunzimea relației oferite prin contactul față în față. Aceste abordări hibride sunt instrumente fiabile în construirea rețelei strategice, ceea ce este de o importanță deosebită pentru grupurile societății civile care doresc să construiască rețele esențiale pentru diplomația publică și colectarea de informații.

IV.2.5. Culegerea de informații și managementul cunoașterii

Managementul cunoașterii este construit proporțional cu capacitatea de colectare și gestionare a datelor și informațiilor culese, indiferent de sectorul de referință, forma sau volumul acestora.

Dacă în cel de-al doilea capitol al tezei am nuanțat formele pe care informația le poate avea, canalele de comunicare prin care aceasta poate fi vehiculată și alte detalii de ordin tehnic, precum raportarea la dimensiunea informației în context digital, în acest capitol accentul este pus pe utilizarea ei în desfășurarea actului diplomatic. Este foarte important de adus în prim plan impactul pe care utilizarea informației digitale îl generează în actualul context de securitate europeană și regională.

În prezent se utilizează diverse mijloacele de colectare a datelor în mediul virtual, specializate pe strângerea de informații din rețelele de socializare, sisteme de comunicații închise (*ex. intranet*) și deschise (*ex. internet, deep-web*). Progresul tehnologic și inovarea în

domeniul „Big Data” au dus la o explozie a tehnologiilor orientate spre producerea de informație și stocarea acesteia în diverse scopuri, dar și spre alternativele de a obține avantaje de pe urma deținătorilor de tehnologie și a beneficiarilor acestora. Astfel, sectoarele cele mai puternic afectate de acest progres sunt protecția datelor personale/ protecția informațiilor clasificate, infrastructurile critice, domeniile cercetării și inovării.

În urma unui studiu din 2010 s-a descoperit că volumul de date produse la nivel global a fost de 1,2 Zettabytes sau 1.200.000.000.000 de trilioane de Gigabyte. S-a preconizat că până la finele anului 2020 volumul mondial de date va ajunge la 35 de Zettabytes. Dorința și capacitatea de a procesa astfel de volume mari de date constituie o componentă semnificativă a definiției „*Big Data*”, dar chiar și în acest context termenul de „*Big Data*” (*trad. Volum Mare de Date*) singur nu este suficient pentru a defini conceptul general de „*Big Data*”.[1]

În aceeași ordine de idei, un alt studiu ne arată că în martie 2019 utilizatorii de internet au produs nu mai puțin de 2,500,000 Terabytes, iar în 2018 utilizatorii din mediul virtual au generat 2.8 milioane ani online.[2]

Dacă ne îndreptăm atenția strict spre utilizarea motoarelor de căutare online, observăm imediat prima și cea mai importantă caracteristică a acestora, anume capacitatea lor de a scala și gestiona miliarde de pagini indexate și dispersate pe Web și aproape instantaneu apare o nevoie de cunoaștere a arhitecturii principale, a elementelor care stau la baza procesului de căutare și extragere și a subsistemelelor de căutare și catalogare - crawling și indexare.[3]

1. Damien van Puyvelde, Stephen Coulthart, Shahriar M. Hossain, „Beyond the buzzword: big data and national security decision-making”, în *International Affairs*, Vol. 93, Nr. 6, 2017, p.1400.
2. Christo Petrov, TechJury, „Big Data Statistics 2019”, 22.03.2019, https://techjury.net/stats-about/big-data-statistics/, accesat în data de 11.08.2019.
3. Stefano Ceri, Alessandro Bozzon, Marco Brambilla, Emanuele Della Valle, Piero Fraternali, Silvia Quarteroni, *Web Information Retrieval*, Edit. Springer, Berlin, Heidelberg , 2013, pp.71-89.

Față de sursele de informații din trecut, înainte de digitalizarea informației, când pentru obținerea unei informații veritabile era nevoie de o adevărată mobilizare de forțe și rețele umane, acum ne regăsim la câteva decenii distanță cufundați într-un ocean informațional, cu resurse incomensurabile și o capacitate limitată de prelucrare a acestora. Identificăm problematici precum: selecția informației alterate, incomplete sau cu scop de dezinformare, verificarea informației reale (nealterate), posibilitatea de verificare și validare a acesteia, identificarea datelor confirmate de natură vitală și de substanță, esențiale împlinirii actului diplomatic. Indiferent de proveniența sau tipul de informație deținut, sistemele de management a informației sunt limitate în principiu de două aspecte: mediile de stocare a informației și capacitatea informatică de procesare a acesteia. Exemplul companiei de telecomunicații australiene Telstra, care utilizează sistemul Splunk[1] în vederea obținerii unui timp de răspuns și acces la volumele mari de date procesate de organizație, centralizat, ne arată faptul că o simplă aplicație informatică care să gestioneze într-un mod eficient și sigur datele nu mai reprezintă o opțiune. Sisteme complexe, precum Splunk, sunt utilizate în construcția sistemelor de securitate cibernetică bazate pe IA și „*machine learning*" sau media.[2]

Inițiativa UE în ceea ce privește IA și Big Data a fost de a aloca un capital financiar total de peste 410 milioane euro în perioada 2014-2020. Acest lucru evidențiază atât interesul uniunii cât și a statelor membre în ceea ce privește progresul tehnologic în procesarea datelor.[3]

1. Spluk.com, Press Release, 2018, https://www.splunk.com/en_us/newsroom/press-releases/2018/telstra-delivers-personalized-customer-experience-with-splunk.html, accesat în data de 11.08.2019.
2. Telstra, „Telstra Global Services Practice", https://www.telstra.com.au/content/dam/tcom/business-enterprise/consulting-services/pdf/telstra-global-services-capabilities.pdf, accesat în data de 11.08.2019.
3. Cécile Huet, Comisia Europeană, „European Commission's Initiatives in Artificial Intelligence", https://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/

Fluxurile de informații la care putem adera prin diverse forme (abonamente, înscrieri la știri zilnice, utilizarea inteligenței artificiale și a tehnologiei „*machine learning*" șamd.) pot fi de real folos atunci când personalul responsabil cu informarea corectă a echipei diplomatice sau, specific, persoana cu atribuțiuni diplomatice, stăpânește arta diplomației și are discernământ diplomatic însoțit de toate calitățile necesare pentru îndeplinirea sarcinilor diplomatice, fie în sectorul diplomației publice, fie în cel guvernamental din arealul cibernetic[1].

În actualul context de securitate, societatea cunoașterii capătă noi valențe și perspective greu, dar necesar de atins. În ceea ce privește lupta împotriva atacurilor aduse sistemului de securitate națională, precum EternalBlue[2], sau observațiite aduse de rapoartele ECFR[3], este necesară demararea unui nou proces de prioritizare și reconceptualizare a sistemului de securitate națională, începând cu pregătirea și formarea reprezentanților instituționali, formatorilor de opinie din sectorul privat, dar și a cetățenilor. După cum reiese din rezultatele cercetărilor unor experți în domeniul securității, „*explozia informațională înseamnă aportul unei cantități imense de date și informații, utile dar și inutile*"[4], motiv pentru care aceasta trebuie gestionată cât mai eficient. Din nefericire, datorită unor limitări trasate de modelele de

conference-agenda/ai-intelligent-machines-smart-policies-huet.pdf, accesat în data de 11.08.2019.

1. Jovan Kurbalija, DIPLO, „25 points for digital diplomacy", 04.11.2016, https://www.diplomacy.edu/blog/25-points-digital-diplomacy, accesat în data de 11.08.2019.
2. Andrew Lipta, „Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems", 25.05.2019, https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity, accesat în data de 11.08.2019.
3. Susi Dennison, Ulrike Esther Franke, & Paweł Zerka, ECFR, 2018, „The nightmare of the dark: The security fears that keep europeans awake at night", https://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n#, accesat în data de 11.08.2019.
4. Babak Bashari Rad, Nafisseh Akbarzadeh, Pouya Ataei, Yasaman Khakbiz, „Security and Privacy Challenges in Big Data Era", în „*International Journal of Control Theory and Applications*", Vol. 9, nr.43, 2016, pp.438-441, https://www.researchgate.net/publication/327111196, accesat în data de 11.08.2019.

guvernanță, securitate și politici, selecția și crearea unei soluții de tipul Big Data, sinteza obiectivă a datelor și informațiilor în vederea obținerii informației vitale poate fi dificil de realizat. Pe de altă parte, resursele financiare și umane ale statelor sunt de cele mai multe ori limitate, motiv pentru care se încheie parteneriate operaționale și strategice sustenabile, de tip public-privat[1]. Pentru a putea satisface nevoile societății cunoașterii în contextul securității naționale, pregătirea și formarea trebuie mult aprofundată și dezvoltată până la împlinirea absolută a nevoilor de intelligence impuse de contextul politic, diplomatic și cel al relațiilor internaționale. Construirea unui curriculum universitar este unul dintre răspunsurile eficiente ale statului la vulnerabilitățile și riscurile identificate în mediul de securitate cibernetic. Un act demn de lăudat este considerentul pe care l-au adoptat și urmat instituțiile de formare a personalului din sectorul de activitate a securității naționale. Aceștia consideră că este *„un obiectiv principal pentru serviciile de informații să creeze programe de formare flexibile pentru educația ofițerilor operativi și analiști. Cheia pentru a reuși o reprezintă asigurarea expertizei all-source, prin absorbția de cunoștințe din diferite domenii”*[2], inclusiv în domeniul securității cibernetice.

Pentru a evidenția nevoia de extragere și prelucrare a informațiilor într-un mod eficient și detașat de sursele de informații și informațiile alterate sau cu o valoare scăzută, se pot aduce în perspectivă utilitatea și utilizarea tuturor disciplinelor de culegere de informații[3], care au un singur țel, obținerea informației vitale. Un caz aparte, cu semnificație în sectorul relațiilor internaționale și în cel diplomatic

1. Parlamentul European, „Legislative Train Schedule - Connected Digital Single Market: Public-Private Partnerships for Cybersecurity”, 20 July 2019, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-public-private-partnerships-for-cybersecurity, accesat în data de 12.08.2019.
2. Cristian Barna, „Pregătire și formare în societatea cunoașterii”, în *Intelligence*, Nr. 35, București, 2017, pp.26-27;
3. HUMINT, GEOINT, MASINT, OSINT, SIGINT, TECHINT, CYBINT/DNINT, FININT.

de asemenea, este cel din 10 aprilie 2018 din Haga, unde s-a pus în aplicare o acțiune sub acoperire din partea Direcției Principale de Activitate a Statului Major General al Forțelor Armate ale Federației Ruse asupra Organizației pentru Interzicerea Armelor Chimice.

Dacă în România, „*actorii din domeniul securității manifestă un interes fundamentat pentru aplicațiile IA, în prezent interesul pentru acest domeniu este unul specific și dedicat. Pentru acest tip de utilizatori este important potențialul noilor tehnologii de a crește capabilitățile de colectare și analiză a datelor. De exemplu, există deja soluții de automatizare a unor sarcini complexe în cazul analizei imaginilor satelitare sau aeriene. Rețele neuronale de tip BGAN (Binary Generative Adversarial Network) realizează operații de segmentare a imaginilor sau identificare a unor detalii specifice.*

În domeniul securității cibernetice există aplicații de tip deep learning dedicate detectării accesărilor neautorizate sau analizei malware. Organizațiile de intelligence sunt preocupate de cunoașterea, prevenirea și contracararea potențialului periculos sau distructiv al tehnologiilor IA. În acest caz pot fi amintite amenințările generate de posibilitatea dublei utilizări a multora dintre tehnologiile IA."[1]

În contextul dezvoltării tehnologiilor, precum realitatea virtuală, mașini inteligente și autonome sau semi-autonome, „*nimeni nu poate nega, impactul pozitiv al tuturor acestor evoluții tehnologice asupra societății, însă nu putem trece cu vederea multitudinea vulnerabilităților care pot fi exploatate și a amenințărilor pe care le pot genera. Pe măsură ce lumea digitală a început să joace un rol principal s-a pus problema securității și a securizării persoanelor și informațiilor personale, a comunicațiilor și a proceselor tehnologice.*"[2]

Cât despre culegerea de informații OSINT, aceasta face parte din instrumentarul general de culegere de informații și este un valoros

1. Cătălin George Vasile, „Inteligența artificială. Între Servicii şi deservicii", în *Revista Intelligence Online*, 04.04.2018, https://intelligence.sri.ro/inteligenta-artificiala-intre-servicii-si-deservicii/, accesat în data de 11.08.2019.
2. Alexandra Stratan, „Proliferarea noilor tehnologii. Inteligența artificială pe câmpul de luptă", în Revista Intelligence Online, 2019.

element din recuzita serviciilor de informații și a organizațiilor private de profil din lumea întreagă.

Natura dinamică și oscilantă în conceptul „*secret-public*" a culegerii de informații din surse deschise este definitoriu expusă în lucrarea „*NATO Open Source Intelligence Handbook*", unde „*OSINT este informația neclasificată, care a fost descoperită deliberat, selectată, filtrată și diseminată pentru o audiență specifică în vederea răspunderii la o anumită solicitare. Aplicate într-un mod sistematic, produsele OSINT pot reduce cererile de colectare a informațiilor secrete, limitând aceste solicitări doar la acele subiecte la care nu se poate oferi un răspuns din surse deschise*"[1]. Tehnicile și metodele de verificare încrucișată și completarea capacităților de culegere de informații din surse deschise cu cele din surse umane de informații - adesea clasificate ca surse secrete de informații - se află în continuare în atenția specialiștilor și experților în studiul de intelligence și în egală măsură este în atenția practicienilor din acest domeniu de nișă. Efectuând o analiză SWOT obiectivă a surselor umane de informații și a surselor deschise de informații, cercetătorii tind să devină imparțiali, deși obiectivul principal ar trebui să fie identificarea modalității optime de fuziune a capacităților și de analiză a datelor culese prin aceste două metode pentru obținerea unui rezultat obiectiv, punctual, clar și fără ambiguitate pentru livrarea către decident, în vederea adoptării celei mai bune soluții.

În ceea ce privește individul, din dorința de afirmare sau de obținere a confortului maxim în relaționare, socializare și comunicare, marea majoritate a acestora se expun gratuit și de foarte multe ori necondiționat în acest vast ocean informațional, unde cei specializați în culegere de informații operează ușor și nedetectați - informațiile și datele culese adesea sunt necesare completării, validării sau verificării informațiilor pe care deja le dețin.

---

1. Theodor Mitu, Daniela Mitu, „OSINT - la granița dintre secret și public", în *Revista Română de Studii de Intelligence*, nr. 4, Edit. Serviciul Român de Informații, București, 2010, pp.42-43.

Pentru a exemplifica și evidenția importanța securizării datelor, care în forma lor brută nu îndeplinesc cerințele minime pentru a fi clasificate în clasa secrete de stat[1], se pot aduce în prim plan două dintre cele mai recente cazuri în care, datorită unor breșe de securitate, datele cu caracter personal ale unor persoane au ajuns în mediul public, iar în urma analizei acestor date au fost identificate persoane care activau în cadrul serviciilor secrete naționale, fapt care a adus o certă atingere securității naționale. Primul caz este cel al Albaniei unde, în 2018, au fost postate pe internet informații sensibile despre ofițeri de informații albanezi, făcându-se referire la identitățile acestora, autovehiculele, rolurile operaționale, delegații, detalii privind misiunile și obiceiurile acestora zilnice, informații care ar fi putut avea consecințe internaționale serioase[2]. Cel de-al doilea caz este din luna iunie 2019, când instituțiile financiare naționale bulgare (NRA) au fost atacate, fiind colectate ilegal informații guvernamentale critice din peste 110 baze de date, care reprezintă aproximativ 3% din dimensiunea datelor gestionate de aceștia. Cu toate că raportul final în ceea ce privește cazul încă nu a fost publicat, s-a raportat faptul că nu au fost compromise informații clasificate, ci doar informații critice[3].

Există o tendință din partea tuturor actorilor - predominant politici - de a da credit, uneori necondiționat, unor surse de informații care și-au demonstrat veridicitatea conținutului informațiilor furnizate în timp. Există un risc care, deși ideologic nu ar trebui să existe, este imperios necesar să fie responsabil asumat, anume orice infor-

1. Art. 15- Art. 19 din LEGEA nr. 182 din 12 aprilie 2002 *privind protecţia informaţiilor clasificate.*
2. Borzou Daragahi, Vincent Triest, „NATO nation Albania publicly posting sensitive intelligence data online -'By getting into Albania's system they can get into NATO's system'", 08.12.2018, https://www.independent.co.uk/news/world/europe/albania-intelligence-data-posted-online-nato-defence-military-finance-security-a8672446.html, accesat în data de 11.08.2019.
3. Angel Krasimirov, Tsvetelia Tsolova, „In systemic breach, hackers steal millions of Bulgarians' financial data", 16.07.2019, https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-hit-bulgaria-send-data-from-russian-email-government-idUSKCN1UB0MA, accesat în data de 11.08.2019.

mație, indiferent de sursa și mediul din care este obținută, trebuie verificată prin mai multe surse, care să-și fi dovedit credibilitate în acest domeniu în trecut. Existența tentației grupurilor societății civile de a urmări sursele care confirmă cel mai bine propria viziune asupra lumii este pe cât de pragmatică pentru formatorii de opinie, pe atât de periculoasă, deoarece poate fi folosită ca metodă de manipulare și dezinformare.

Indiferent de libertatea de exprimare a presei, tehnicile de „cenzură modernă" a fluxurilor de informații sunt utilizate peste tot în lume și poate fi extrem de dificil de identificat în numele cărui stat ar putea să opereze. Unele guverne, în special Rusia și China, au profitat de aceste tipuri de gestionare a informației în mediile virtuale cu ajutorul multor instrumente, printre care formarea unor formatori de opinie cărora le-au crescut credibilitatea în rândurile populației. Metodele utilizate de acești indivizi se regăsesc, din punct de vedere procedural, în sectorul de practică al ingineriei sociale, domeniu care este adesea ridicat la rang de artă și considerat a fi unul dintre cele mai puternice instrumente din arsenalul oricărei forme de guvernământ moderne.

RT[1] [2], principalul furnizor de știri rusofone în limba engleză și totodată una dintre cele mai importante posturi de televiziune internaționale, este de fapt o operațiune extrem de sofisticată prin care se transmite viziunea Moscovei asupra evenimentelor în lumea întreagă. În general, trusturile media au fost doar niște instrumente, un tip de expresie a dezbaterii publice mai degrabă decât un actor independent. Accesul la canalele mass media a fost inegal şi câteodată distorsionat. Înfometarea şi violența, cataclismele, dezastrele, explozivul, extraordinarul sunt, de regulă, subiecte mai acaparante decât negocierile pentru pace. Cu toate acestea, actorii societății civile care

1. Madalin Voicu, *Matrioșka mincinoșilor. Fake news, manipulare, populism*, Editura Humanitas, București, 2018, p. 177.
2. RT, https://www.rt.com/, accesat în data de10.08.2018.

au învățat să folosească eficient resursele media au avut capacitatea de a-şi face cunoscută perspectiva cu o eficiență mai ridicată[1]. Mai puțin nuanțat, Moscova angajează o armată de bloggeri sau vloggeri pentru a participa la dezbateri online, în special pe temele de discuții din știri și din secțiunile de comentarii ale ziarelor occidentale. Este o adevărată provocare să se facă distincția între un blogger pro-rus și un comentator occidental cu o viziune mai nuanțată asupra relațiilor Occidentului cu Rusia. Guvernele occidentale urmăresc, de asemenea, fluxurile informaționale virtuale pentru a înțelege reacțiile publice, inclusiv reacțiile sectorului public străin, la inițiativele lor politice sau la o prognoză a efectelor acestora în viitorul apropiat. Acest lucru înlocuiește din ce în ce mai mult sondajele și alte tehnici de analiză a opiniei publice care au fost utilizate de la începutul mileniului pentru a evalua reputația și marca națională. Acest lucru se aplică atât opiniei naționale, cât și opiniei internaționale. Unii comentatori au sugerat că monitorizarea sectorului social online ar putea înlocui sondajele de opinie privind alegerile locale/naționale.

Rețelele de socializare online, se pot într-adevăr extinde asupra unui eșantion mai larg, fără a ține cont de granițele geografice și se pot întinde până în mediul internațional. În acest caz, problema este legată de selecția persoanelor sub semnul obiectivismului. În mod tradițional, rezultatele sondajelor și intervievării grupurilor de contacte sunt selectate cu mare grijă, existând astfel un control asupra rețelelor sociale, indiferent de forma acestora. Prin aplicarea acestui model tradițional, colectorul de informații, sau probabil sociologul, va putea oricând să solicite lămuriri asupra afirmațiilor obținute în urma unei întâlniri de lucru, pe când în mediile sociale online nu există această posibilitate, de cele mai multe ori reacția este scurtă, subiectivă, bazată pe o emoție de moment, care poate sau nu poate fi asociată unui tipar de gândire.

1. Mary Kaldor, *Securitatea Umană*, Edit. CA Publishing, Cluj-Napoca, 2010, p.50.

Instrumentele digitale, în mod uzual, nu oferă doar modalități de colectare a informațiilor despre evenimente și percepții publice, acestea având și capacitatea de analiză a acestor informații și gestionarea cunoștințelor și înțelegerii astfel generate. Acest lucru este deosebit de important pentru guvernele statelor europene și grupurile societății civile, care nu dispun de o capacitate de analiză internă (națională) semnificativă. Monitorizarea atentă a mediilor sociale, de exemplu Facebook, Instagram, Twitter, LinkedIn șamd., poate ajuta la identificarea analiștilor în anumite domenii, fie ele tematice sau generale. Această activitate permite actorilor diplomatici să citească blogurile și alte analize online publicate de analiști, având chiar și posibilitatea de a păstra un contact direct ca formă de verificare a credibilității acestora și autenticității informațiilor sintetizate și furnizate de aceștia. Din punct de vedere tehnico-tactic, contextul este cheia, acesta este de regulă pregătit prin analizarea numărului de distribuiri, comunitățile sau grupurile în care această informație este distribuită, numărul de persoane ce aprobă prin „*like*" sau dezaprobă prin „*dislike*" această informație, comentariile aduse la postările online și de asemenea modificările aduse la acestea, formularea acestor postări, publicul țintă pentru care este conceput, reacția publică, precum și segmentarea persoanelor care au interacționat sub o formă sau alta la aceste postări.

În secțiunea destinată înțelegerii rețelelor astfel de abordări online pot atinge maximum de eficiență dacă se regăsesc în strategiile hibride alături de abordările tradiționale, relaționarea interpersonală. În cazul analiștilor, rețelele de socializare online preced invitațiile de participare la conferințe sau grupuri de lucru în vederea înțelegerii și aprofundării temelor de interes comun, care pot fi apoi urmate de continuarea relațiilor online și crearea sau extinderea de comunități profesionale. Platformele sociale, conform Figurii nr. 6, pot fi utilizate pentru a crea forumuri, grupuri (deschise, private, secrete, hibride) și alte forme de interacțiune online cu profesioniști, diverși formatori

de opinie, oameni politici, membri ai comunităților profesionale și activiști sau persoane interesate de diverse teme de discuții.

Totuși, acesta este un exemplu în care inovarea digitală ar trebui să poată crea platforme mai adaptate la nevoia de metode analitice on-line. Wikistrat[1] este o organizație orientată spre consultanță geopolitică cu surse globale. Aceasta i-a permis formarea unei platforme digitale în parteneriat cu peste 2200 de experți din întreaga lume, care participă la simularea de scenarii și exerciții de grup sau forumuri cu dezbateri tematice.

Platforma este concepută astfel încât să ofere recompense și stimulente analiștilor pentru a participa, precum și pentru a permite echipelor de management să exerseze și să modereze dezbateri.

Exercițiile sunt fie lansate la solicitarea unui client, caz în care clientul cumpără forma finală a raportului, fie sub forma unor exerciții cu teme generale, caz în care rapoartele sunt puse la dispoziția analiștilor participanți și uneori a publicului larg. Exercițiile generale permit analiștilor să-și îmbunătățească abilitățile analitice în timp ce fac schimb de informații și surse între ei și totodată permit Wikistrat să identifice cei mai buni analiști care pot fi utilizați în cadrul exercițiilor orientate pe nevoile clienților. Astfel, Wikistrat are în portofoliu un număr foarte mare și divers de analiști, chiar mai mult decât sperau să obțină la implementarea proiectului. Acest tip de platformă, chiar dacă la o scară mai mică, dar care se concentrează exclusiv pe un număr mic de analiști identificați, evaluați și de încredere, oferă guvernelor sub-naționale și grupurilor societății civile perspectiva unei schimbări treptate a capacităților lor analitice. Acesta este doar un exemplu în care inovația în designul platformelor specializate de acest tip poate aduce rezultate considerabil mai mari decât cele disponibile prin instrumentele oferite de rețelele sociale din mediul online.

1. http://www.wikistrat.com/, accesat în data de 27.08.2018.

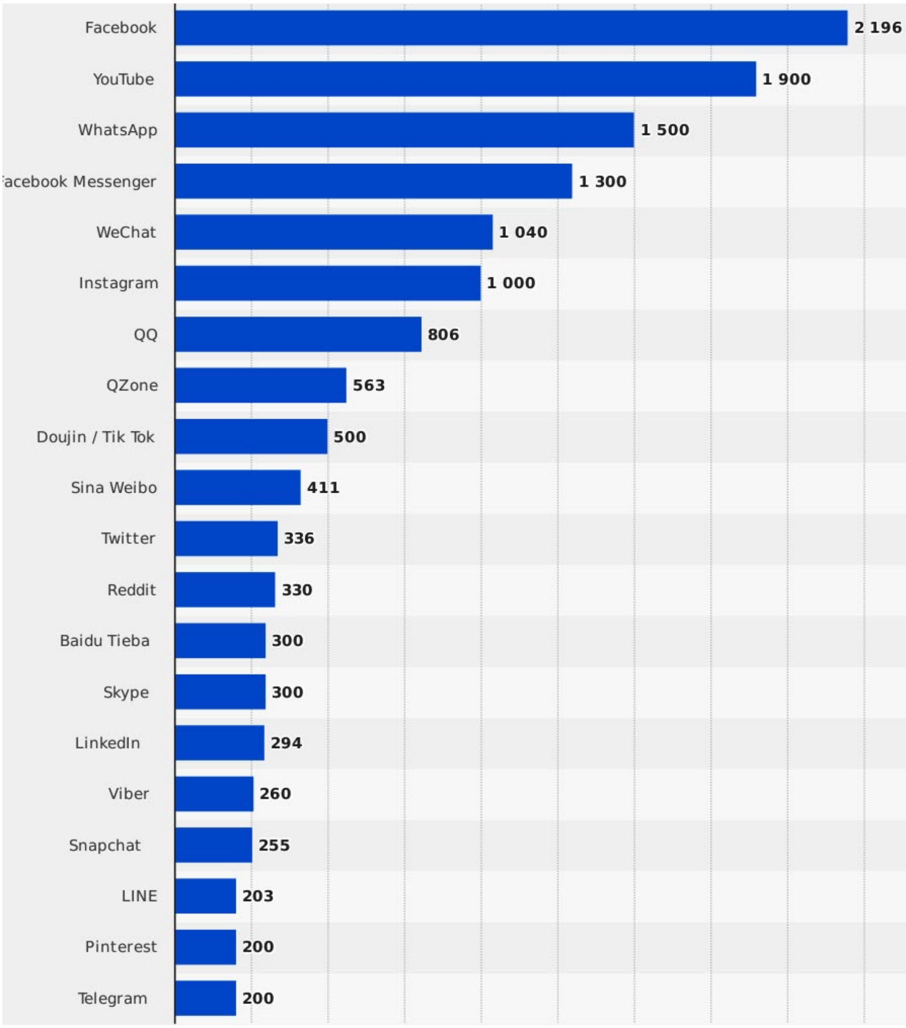


Figura nr.20. Cele mai renumite instrumente de socializare online din întreaga lume (iulie 2018), reprezentate în baza numărului de utilizatori activi (în milioane)[1]

1. „Most famous social network sites worldwide as of July 2018, ranked by number of active users (in millions)", https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/, accesat în data de 27.08.2018.

IV.3. Securitate diplomatică și guvernare prin reziliență cibernetică

Conceptul securității diplomatice apare în contextul protejării intereselor naționale în momentele de criză și instabilitate, dar și în cel al valorificării oportunităților de întărire a poziției statului în interiorul comunității internaționale. Acest concept vine ca răspuns la nevoia de aliniere la sistemele diplomatice și normele internaționale, la așteptările regionale sau comunitare și la interesele statelor cu care statul are o relație bazată pe interese naționale. Aceste interese nu sunt împlinite mereu din partea statelor ori a comunității internaționale, motiv pentru care este necesară înțelegerea unei abordări reziliente și prin mijloacele moderne din sectorul cibernetic.

Securitatea diplomatică există în primul rând prin adoptarea de normative prin convenții, tratate, ratificarea de acorduri și adoptarea acestora în legislația națională, păstrând totodată caracterul suveran al statului.

IV.3.1. Evoluția rezilienței cibernetice ca efect al politicilor de securitate diplomatică

Odată cu documentul care reglementează dintr-o perspectivă strategică securitatea cibernetică a UE, emis în 07 februarie 2013, s-au pus bazele a ceea ce înseamnă implicarea UE în consolidarea capacităților informatice externe, fapt care a consolidat abordarea strategică a UE în spectrul internațional.

Concluziile Consiliului, care a avut loc în 11 februarie 2015 la Bruxelles, privind diplomația cibernetică au consolidat ideea necesității cooperării internaționale și asistenței în domeniul construirii și dezvoltării capacităților cibernetice pentru a întări toate ariile securității din mediile virtuale și a lupta împotriva criminalității cibernetice. Principalele aspecte evidențiate în Concluziile Consiliului includ:

- *„Dezvoltarea unei abordări coerente și globale pentru consolidarea capacităților cibernetice, care, pe de o parte, să reunească tehnologia, politicile și dezvoltarea competențelor în cadrul unei agende a UE mai complexe și cuprinzătoare privind dezvoltarea și securitatea, și, pe de altă parte, să faciliteze conceperea unui model eficace al UE pentru consolidarea capacităților cibernetice;*
- *Integrarea creșterii capacităților cibernetice în abordările globale mai cuprinzătoare din toate domeniile spațiului cibernetic, inclusiv printr-o strânsă cooperare cu mediul academic și sectorul privat, precum și cu Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), cu Centrul european de combatere a criminalității informatice din cadrul Europol și cu Institutul pentru Studii de Securitate al UE;*
- *Să acorde sprijin noilor inițiative privind consolidarea capacităților cibernetice care iau în considerare, au la bază și completează inițiativele existente, subliniind importanța accesului la TIC deschise și sigure și a utilizării nerestricționate, necenzurate și nediscriminatorii a acestora, pentru favorizarea unor societăți deschise și crearea de condiții pentru creștere economică și dezvoltare socială;*
- *Promovarea consolidării durabile a capacităților cibernetice, atunci când este cazul, împreună cu parteneri internaționali, precum și simplificarea și stabilirea priorităților în ceea ce privește finanțarea, inclusiv prin utilizarea pe deplin a instrumentelor financiare externe și a programelor relevante ale UE;*
- *Promovarea pe plan internațional a Convenției Consiliului Europei privind criminalitatea informatică drept cadru juridic de referință pentru cooperarea internațională în combaterea criminalității informatice la nivel mondial și să sprijine țările terțe să adere la convenție și să introducă un cadru național juridic minim de combatere a criminalității informatice, precum și să dezvolte capacitățile necesare de anchetă și urmărire penală;*

- *O abordare asupra amenințărilor și provocărilor tot mai mari din domeniul cibernetic prin creșterea rezilienței infrastructurii critice de informație prin consolidarea cooperării strânse și a coordonării în rândul părților interesate la nivel internațional, prin inițiative precum consolidarea încrederii, elaborarea unor standarde comune, exerciții cibernetice la nivel internațional, sensibilizare, formare, cercetare și educație, mecanisme de reacție la incidente;*
- *Valorificarea cunoștințelor de specialitate ale organizațiilor naționale din domeniul cibernetic, inclusiv ale echipelor de intervenție în cazul producerii unor incidente care afectează securitatea informatică, ale unităților de combatere a criminalității din domeniul înaltei tehnologii și ale altor organisme naționale competente, în alte cuvinte creșterea rezistenței prin dezvoltarea capacităților și a competențelor, mobilizarea expertizei organizațiilor cibernetice naționale (cum ar fi CERT / CSIRT-uri, unități de criminalitate de înaltă tehnologie etc.)"*[1].

Această poziție a fost readoptată și reiterată în 2017[2], poziție care recunoaște eforturile CCB, contribuie la îndeplinirea angajamentelor de dezvoltare ale UE și la creșterea nivelului securității cibernetice la nivel global.

În 2015, Consiliul, prin Formațiunea Afaceri Generale a Consiliului (CAG), a emis în vederea adoptării actul/anexa oficială privind Diplomaţia Cibernetică Europeană „*An outline for European Cyber Diplomacy Engagement*", care aduce în prim plan modalitatea de raportare a diplomației cibernetice la progresul și evoluția tehnologică în sectorul relațiilor internaționale.

1. Comisia Europeană, Înaltul Reprezentant al Uniunii pentru Afaceri Externe și Politica de Securitate, Secretariatul General al Consiliului, 6122/15, „Concluziile Consiliului privind diplomația cibernetică" din 13 septembrie 2017, p.2.
2. „Comunicare Comună către Parlamentul European și Consiliu - Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE".

IV.3.2. Provocările Agendei UE în contextul securității cibernetice

Provocările privind spațiul cibernetic au devenit un element central al agendei externe a UE, iar acest lucru s-a datorat numărului tot mai mare de raportări din partea forurilor internaționale care abordează diverse aspecte legate de spațiul cibernetic, regularizarea acestuia prin angajamente și normele de conduită și comportament în spațiul cibernetic, aplicabilitatea statului de drept în ceea ce privește legea drepturilor omului în spațiul cibernetic (*Liniile Directoare ale UE privind Drepturile Omului asupra Libertății de Expresie online şi offline*), securitatea informatică, consolidarea capacităților și guvernarea internetului prin promovarea Convenției de la Budapesta[1] ca model pentru dezvoltarea legislației naționale[2] în domeniul criminalității cibernetice şi ca bază pentru o cooperare internațională pe termen lung. Uniunea Europeană și întreaga sa componență a jucat un rol-cheie în sectorul relațiilor internaționale, aducând plusvaloare în majoritatea dezbaterilor și realizărilor politicii internaționale în materie de valorificare a resurselor cibernetice până în prezent.

Cu ocazia CAE din 19 iunie 2017 de la Luxemburg au fost adoptate Concluziile Consiliului privind "*Cyber diplomacy toolbox*[3]", prin care UE obține dreptul de a impune sancțiuni, desigur financiare, făptuitorului - persoană fizică, persoană juridică sau stat - care desfășoară activități ostile și de atac asupra rețelelor informatice ale organizațiilor

1. Consiliul Europei, „Convention on cybercrime" din 23 noiembrie 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, accesat în data de 03.03.2019.
2. Legea nr.64 din 24 martie 2004 p*entru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001*, M.Of. nr. 343/20 apr. 2004 modificată de Legea nr.105 din 14 aprilie 2009 *pentru ratificarea Protocolului adiţional, adoptat la Strasbourg la 28 ianuarie 2003, la Convenţia Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă şi xenofobă săvârşite prin intermediul sistemelor informatice*, M.Of. nr. 278/28 apr. 2009.
3. Erica Moret, Patryk Pawlak, Brief SSUE, 24/2017, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?", *https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf, accesat în data de 04.03.2019;*

naționale și supranaționale din blocul comunitar. Această măsură a fost anunțată de miniștrii de externe ai UE. Aceasta reprezintă o măsură coercitivă necesară a blocului comunitar pentru descurajarea atacurilor cibernetice sau înlesnirii infracțiunilor informatice. Măsura a fost adoptată după o atentă analiză a evenimentelor și incidentelor cibernetice survenite pe teritoriul UE[1]. Cu această ocazie, UE, prin miniștri de externe, a hotărât care sunt aceste măsuri restrictive - interdicții de călătorie, blocarea activelor și până la imposibilitatea de a derula afaceri cu o persoană, organizație sau guvern al unui stat membru UE. După cum a mai fost menționat, răspunsul organismelor specializate în identificarea activităților infracționale din arealul cibernetic trebuie să fie unul prompt și direct proporțional cu elementele constitutive ale raportului privind atacul cibernetic -sectorul afectat, complexitatea și dimensiunea atacului, durata și impactul atacului sau a activității cibernetice.

Deși noile tendințe, noul cadru legislativ european, apariția noilor instituții supranaționale și noile inițiative ale UE recunosc capacitatea și resursa inestimabilă a arealului cibernetic cu oportunități în sectorul coeziunii economice și sociale, acestea recunosc și existența unor provocări care au apărut în mod natural și a altor provocări care au apărut într-un mod sintetic și într-un stadiu evolutiv continuu. Aceste din urmă provocări sunt o limitare aplicată acțiunii externe a UE. În acest context, nu este o noutate exprimarea îngrijorării de către UE cu privire la capacitatea și disponibilitatea celorlalți actori - statali și nestatali- în atingerea scopurilor impuse de politica de stat sau de motivațiile politice ori economice cu ajutorul instrumentarului digital în mediu cibernetic. Desigur, în tratarea acestei problematici legislația există și poate fi asumată pentru crearea unui răspuns comun la nivelul UE. În acest context legislativ, UE conștientizează statele membre cu privire la permisivitatea și lipsa de implicare

1. AGERPRES, „https://www.agerpres.ro/externe/2017/06/19/ue-a-convenit-sa-impuna-sanctiuni-hackerilor-care-ataca-retele-informatice-ale-statelor-membre-13-19-19", accesat în data de 04.03.2019.

asupra utilizării spațiului cibernetic pe teritoriul național în favoarea actelor ilicite și sancționarea acestora - atacatorilor și a facilitatorilor.

Cadrul privind un răspuns diplomatic comun al UE face parte din abordarea acesteia în ceea ce privește diplomația cibernetică. Acest cadru vine în sprijinul aplanării situațiilor preconflictuale, cu un potențial în diminuarea sau dizolvarea amenințărilor în context de securitatea cibernetică și desigur pentru obținerea unui raport sustenabil de stabilitate în domeniul relațiile internaționale cu statele din vecinătatea UE sau cu marile puteri. Încurajarea și facilitarea unui cadru de cooperare internațional este se numără printre interesele primare ale UE pe termen scurt și lung.

Astfel, *„UE își reafirmă angajamentul față de soluționarea diferențelor internaționale din spațiul cibernetic prin mijloace pașnice. În acest context, toate eforturile diplomatice ale UE ar trebui, cu titlu prioritar, să vizeze promovarea securității și a stabilității în spațiul cibernetic prin intensificarea cooperării internaționale și reducerea riscului de percepție eronată, de escaladare și de conflict care ar putea apărea în urma incidentelor din domeniul TIC."*[1]

În ceea ce privește Agenda Digitală Europeană, strategia pentru o piață digitală a fost finalizată și ratificată de Comisia Europeană, fiind comunicată oficial în luna mai 2015 și prezentată în cadrul întâlnirii Consiliul European din luna iunie 2015. Totodată, în contextul dezvoltării, inovării și susținerii securității cibernetice în plan european au fost prezentate și propunerile în vederea consolidării parteneriatelor public-privat. Acest parteneriat[2] s-a materializat în

1. Consiliul European, Comunicat de presă, 19/06/2017, „Atacurile cibernetice: UE este pregătită să reacționeze printr-o serie de măsuri care includ sancțiuni", https://www.consilium.europa.eu/ro/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/, accesat în data de 04.03.2019.
2. Parlamentul European, Piața Unică Europeană, „Commission signs agreement with cybersecurity industry to increase measures to address cyber threats", 5 iulie 2016, https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats, accesată în data de 04.03.2019.

5 iulie 2016 printr-un contract de parteneriat public-privat /cPPP privind securitatea cibernetică.

Odată cu abordarea acestei noi optici, UE poate realiza investiții la o scară mult mai mare și are nevoie de un mecanism mai eficace care i-ar permite să construiască capacități durabile, să pună în comun eforturi și competențe și să stimuleze dezvoltarea de soluții prin inovare, care să răspundă provocărilor industriale în materie de securitate cibernetică în domeniul noilor tehnologii multiple (*de exemplu inteligența artificială, informatica cuantică, tehnologia blockchain și identitățile digitale sigure*), precum și în sectoarele critice (de exemplu transporturi, energie, sănătate, finanțe, guvernare, telecomunicații, producție, apărare, sectorul spațial).

Comunicarea comună a avut în vedere posibilitatea consolidării capacității UE în domeniul securității cibernetice, prin intermediul prezentei politicii de coeziune a UE și a următoarei politici pentru intervalul 2021-2027, a unei rețele de centre de competențe, având drept coordonator un centru european central cu expertiză în acest domeniul.

Aceasta ar urmări să completeze eforturile existente de consolidare a capacităților în acest domeniu la nivelul organismelor supranaționale ale UE și la nivelul sistemelor naționale în calitate de furnizori de securitate. În comunicarea comună s-a făcut cunoscută intenția Comisiei de a lansa, în 2018, o evaluare a impactului pentru a examina opțiunile disponibile în vederea instituirii acestei structuri. Ca un prim pas și pentru a colecta informații utile pentru abordările viitoare, Comisia a lansat, în cadrul programului Orizont 2020, o fază pilot, care să ajute la reunirea centrelor naționale într-o rețea care să impulsioneze dezvoltarea competențelor și dezvoltarea tehnologică în materie de securitate cibernetică.

În cadrul summitului digital de la Tallinn, din septembrie 2017, șefii de stat și de guvern au cerut Uniunii să devină *„un lider mondial în domeniul securității cibernetice până în 2025, pentru a asigura încrederea și protecția cetățenilor, a consumatorilor și a întreprinderilor online și pentru a permite un internet liber și reglementat juridic*."

Concluziile Consiliului, adoptate în 20 noiembrie 2017, au invitat Comisia să prezinte rapid o evaluare a impactului cu privire la opțiunile posibile și să propună, până la jumătatea anului 2018, instrumentul juridic relevant pentru punerea în aplicare a inițiativei.

IV.3.2. Programul Europa digitală, un nou orizont, o nouă abordare

Programul Europa digitală, propus de Comisie în luna iunie 2018[1], urmărește să extindă și să maximizeze beneficiile transformării digitale pentru cetățenii și întreprinderile europene în toate domeniile relevante ale politicilor UE, consolidând politicile și sprijinind obiectivele ambițioase ale pieței unice digitale. Programul propune o abordare coerentă și globală în vederea asigurării unei utilizări optime a tehnologiilor avansate și a combinației adecvate de capacitate tehnică și competență umană pentru transformarea digitală - atât în sectorul securității cibernetice, cât și în domeniile de infrastructură de date inteligente, inteligență artificială, competențe și aplicații avansate în industrie și în domeniile de interes public. Aceste elemente sunt interdependente, se susțin reciproc și, atunci când sunt încurajate simultan, pot atinge nivelul necesar pentru a permite succesul economiei datelor.[2] Programul Orizont Europa[3]- următorul program-cadru

1. Comisia Europeană, COM(2018) 434 final, 06.06.2018, „Regulament al Parlamentului European și al Consiliului de instituire a programului Europa digitală pentru perioada 2021-2027", http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-434-F1-RO-MAIN-PART-1.PDF, accesat în data de 04.03.2019.
2. Draftul de lucru al Comisiei Europene, „COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027", https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52018SC0305&from=EN, accesat în data de 04.03.2019;
3. Comisia Europeană, „Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de instituire a programului-cadru pentru cercetare și inovare Orizont Europa și de stabilire a normelor sale de participare și de diseminare (Text cu relevanță pentru SEE)", http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-435-F1-RO-MAIN-PART-1.PDF, accesat în data de 04.03.2019.

pentru cercetare și inovare al UE - include, de asemenea, *securitatea cibernetică în rândul priorităților sale.*

În această ordine de idei, deputații din cadrul Parlamentului European au adoptat, în 12.03.2019, la Strasbourg, legea securității cibernetice în circumscripția UE, care atestă prima formă de certificate la nivelul UE, cu scopul de a asigura beneficiarii că serviciile prestate, procesele derulate și produsele comercializate în zona UE sunt conform standardelor de calitate minime în sectorul de securitate cibernetică. Totodată, în Parlamentul European s-a votat o rezoluție care promovează o acțiune la nivel european în ceea ce privește amenințările de securitate legate de prezența tehnologică crescută a echipamentelor produse în China pe teritoriul Uniunii Europene. Cu această ocazie, s-a exprimat unanim îngrijorarea în ceea ce privește acuzațiile potrivit cărora echipamentele de telecomunicații compatibile cu tehnologia 5G ar putea avea sau chiar au încorporate soluții de tipul „*back-door*", care pot permite cu ușurință producătorilor de tehnologie chinezi şi autorităților chineze - *guvernului* - accesul neautorizat pentru a culege date cu caracter personal şi metadate din sistemele și rețelele existente pe teritoriul UE[1].

Așadar, concentrându-ne atenția asupra incidenței aparatului legislativ european în România, putem spune că segmente din „*obiectivele stabilite de Agenda digitală europeană au fost preluate şi adaptate la contextul actual din România, în măsura în care acestea sunt relevante şi aliniate la viziunea strategică TIC a României pentru perioada 2014 - 2020"*[2] în cadrul Strategiei Naționale privind Agenda Digitală[3] pentru

1. Parlamentul European, 2017/0225(COD), „EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)" https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0225(COD)&l=en, accesat în data de 12.03.2019.
2. Ministerul Comunicațiilor și Societății Informaționale, „Agenda Digitală pentru România 2020", https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/Strategia-Nationala-Agenda-Digitala-pentru-Romania-2020-aprobata-feb-2015.doc, accesat în data de 04.03.2019.
3. Ministerul Comunicațiilor și Societății Informaționale, „Agenda Digitală pentru România 2020", https://www.comunicatii.gov.ro/agenda-digitala-pentru-romania-2020/, accesat în data de 04.03.2019.

România. *„Una din acțiunile care trebuie întreprinse în cadrul Agendei Digitale se referă la consolidarea încrederii şi a securității online, Europa având nevoie de consolidarea politicii de combatere a criminalității informatice, a pornografiei infantile online şi a nerespectării vieţii private şi a datelor cu caracter personal. SM UE trebuie să ia măsuri pentru introducerea unei rețele performante la nivel național şi să pună în aplicare simulări de atacuri cibernetice la scară largă”.*[1] *„Platformele naționale de alertă trebuie adaptate la platforma de combatere a criminalității cibernetice a Europol”.*[2]

„Agenda digitală pentru România este constituită dintr-un grup de inițiative, dintr-un grup de dosare şi se află în desfășurare pe mai multe componente. Toate fac parte din ceea ce numim eGovernment[3]. *Sunt demersuri de mare anvergură, ce presupun finanțări europene. Partea de Cloud guvernamental*[4] *este un proiect care a pornit ca şi inițiativă acum câțiva ani, dar undeva în primăvara acestui an se va finaliza studiul de fezabilitate după care va intra în procesul de finanțare efectivă. Cred că în România există foarte multă inițiativă din diferite părți ale administrației statului pentru creșterea nivelului de digitalizare. De fapt, agenda digitală, acesta este rolul ei în principiu, să aducă la o congruență toate aceste inițiative şi tot acest efort într-un punct unic de tracțiune, astfel încât să putem asambla toate aceste demersuri şi împreună să creștem gradul de digitalizare al României. Există orașe care au un nivel de digitalizare mai ridicat, deja cochetează cu conceptul de Smart, altele puțin mai progresive,*

1. Ministerul Afacerilor Externe, Securitate cibernetică, „Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora”, https://www.mae.ro/node/28369?page=3, accesat în data de 07.03.2019.
2. Comunicare a Comisiei din 19 mai 2010 către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor intitulată „O Agendă digitală pentru Europa”, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:si0016&from=RO, accesat în data de 07.03.2019.
3. Comisia Europeană, „European eGovernment Action Plan 2016-2020”, https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020, accesat în data de 12.03.2019.
4. Ministerul Comunicațiilor și Societății Informaționale, „Cloud-ul guvernamental, un beneficiu pentru instituţii”, 30.08.2018, https://www.comunicatii.gov.ro/cloud-ul-guvernamental-un-beneficiu-pentru-institutii/, accesat în data de 12.03.2019.

dar nu atât de rapide în adopția noilor tehnologii. Văd că se poate şi încep la rândul lor să se facă pași îndrăzneți pe această cale."[1]

IV.3.4. Paradigma diplomației securității cibernetice

Diplomația cibernetică, fundamental, se poate rezuma și la înțelegerea celui mai eficient mod de comunicare și finalmente de obținere a deciziei favorabile instituției pe care decidentul o reprezintă și implicit a statului sub egida căruia activează.

Acest prim cuvânt cheie „*înțelegere*" sau „*cunoaștere*", utilizat într-un cadru activ, este esențial în practicarea oricărui tip de diplomație, deoarece însăși nevoia acestei onorabile profesii se naște din nevoia de a înțelege diversele culturi și societăți în plan național, internațional și chiar în plan global. Se accentuează nuanțele principiului de a găsi asemănările între aceste forme sociale pentru obținerea celor mai bune rezultate în parteneriat cu acestea. Găsirea unui teren neutru sau a unui mijloc ideal de obține aceste rezultate este extraordinar de dificilă.

În sectorul cibernetic, utilizând mijloacele și resursele mai sus menționate, identificăm un număr de trei modalități de practică a diplomației cu și prin intermediul spațiului cibernetic.

A. *Colectarea și strângerea de informații*

Această muncă de strângere de informații pentru a obține o informație vitală de o importanță deosebită trebuie să fie bazată pe un spirit critic și o viziune obiectivă, realistă. Informațiile se regăsesc peste tot în jurul nostru, dar capacitatea de a le culege din cele mai veritabile surse de date și informații este cea mai valoroasă. Din cele mai des întâlnite metode de culegere de informații, consider metodele de granularitate cele mai eficiente. Orice informație are o anumită

1. Interviu din 03.03.2019 pentru MEDIAFAX cu ministerul MCSI, domnul Alexandru Petrescu, https://www.mediafax.ro/economic/interviu-ministrul-comunicatiilor-intentia-e-sa-avem-licitatia-pentru-5g-in-2019-ce-spune-despre-oug-114-17896378, accesat în data de 12.03.2019.

valoare, iar valoarea aceasta depinde de modalitatea de valorificare a celui ce a obținut-o. Urmărind și chiar monitorizând, cu sprijinul mijloacelor avute la dispoziție (ex. OSINT) și printr-o simplă analiză și sinteză a factorilor generatori de date și informații, în vederea obținerii informației esențiale, se pot obține avantaje de timp și de resurse extraordinare. Fluxurile informaționale sunt din ce în ce mai complexe, unele chiar exclusiviste, iar facilitarea accesului în anumite grupuri de informări și comunicări este dificilă. Cu toate acestea, vin în ajutor organismele naționale și internaționale sau comunitățile specializate în această arie de interes.

Scopul acestui proces este unul evident, de a utiliza resursele rezultate în îndeplinirea obiectivelor, care nu ar putea fi atinse în lipsa acestora.

B. *Monitorizare activă*

A doua modalitate este de adoptare de strategii de monitorizare activă a fluxurilor informaționale pentru încropirea de relații diplomatice cu factorul de decizie sau influență dintr-un anumit sector. Monitorizarea, în acest caz, nu se referă la o ascultare activă, precum ascultarea pentru a învăța și ascultarea pentru a înțelege informația, este mai mult de atât, se referă la preluarea informațiilor, trunchiate chiar, prin diverse canale de comunicații (audio, video, text șamd.) și analizarea acestora în vederea obținerii unei informații complete asupra poziției sau mesajului celui ce a comunicat aceste date.

C. *Resurse umane de informații*

Cea de-a treia modalitate este prin utilizarea resurselor umane ca mijloc de obținere a datelor și informațiilor necesare. Acest lucru poate fi făcut prin integrarea ca membru activ (uneori chiar pro-activ) în grupuri, comunități, rețele de informații și alte zone punctual, respectiv contextual alese pentru obținerea celei mai bune informații. Atuul în sectorul virtual este că modalitatea de integrare în aceste comunități nu mai este reglementată sau limitată de formă, ci de prestigiu și de valoarea de piață.

Concluzii preliminare

Diplomația evoluează continuu, iar în ultimii 50 ani progresul tehnologic a forțat statele să regândească conceptul și actul diplomatic. Aplicând metoda observației asupra sectorului politic contemporan, vom observa fără mari dificultăți cum orice informație cu impact în domeniul relațiilor internaționale și de securitate al statelor devine publică aproape instant, iar protagoniștii acestor diseminări sunt chiar diplomații și personalul consular. Unul dintre experimentele făcute pentru a-mi susține și întări ipoteza a fost dat de urmărirea în timp real a trei surse de informații, care în mod direct nu aveau nici o legătură și totuși au avut rezultatul intuit de mine, respectiv una din piețele bursiere internaționale, un canal de știri care furnizează transmisii în direct și presa online. Deși se zvoneau și se speculau anumite vești, care încă nu fuseseră lansate oficial, la câteva secunde după emiterea din partea unui decident politic român a unei frânturi de informație (prognozată de analiști de bursă) și apariția aproape instant a acelui moment pilot în presa online, bursa pe un anumit sector s-a modificat brusc, fără ca o mașinărie financiară să își facă simțită prezența. Evident, după lansarea întregii informații în context oficial, bursa s-a redresat, însă răul era deja făcut.

În mod evident, o simplă afiliere cu un anumit actor politic pe Facebook sau un tweet cu frânturi de informație pot duce nu doar la instabilitatea unui preț pe bursă, ci la instabilitatea economică sau de securitate a unei țări.

În România până în acest moment nu am identificat o analiză a acestui subiect, motiv pentru care elementele de noutate sunt date de studierea atât a diplomației digitale, cât și a diplomației cibernetice în raport cu noul context de securitate național, european și de ce nu global. Dezvoltarea subiectului a dus la înțelegerea noului instrumentar diplomatic cu elemente ce țin de arealul cibernetic și

utilizarea acestuia în raport cu respectarea și aplicarea, în continuare a protocolului diplomatic tradițional.

Apariția diplomației publice și digitale a fost determinată de intrarea unor noi actori, atât guvernamentali cât și non guvernamentali, în mediul internațional, de dezvoltarea unei noi agende internaționale de securitate și facilitată de noile tehnologii informatice și de comunicații. Toate acestea sunt instrumente importante care își fac simțit aportul în sprijinul unor strategii diplomatice mai largi. Acestea sunt cu adevărat eficiente atunci când sunt integrate în strategii mai largi destinate să asigure obiective naționale (în cazul guvernelor) sau obiective organizaționale (în cazul ONG-urilor sau grupurilor societății civile). Atunci când nu are ca scop imediat obiective strategice clare, diplomația publică riscă să fie redusă la o dimensiune mai banală, în timp ce diplomația digitală devine prin prezența sa în sectorul mass-media și a rețelelor de socializare online aproape o obsesie. De cele mai multe ori, acestea subminează într-o oarecare măsură credibilitatea actorilor diplomatici implicați în actul diplomatic internațional și, prin urmare, capacitatea acestora de a-și îndeplini obiectivele strategice. În sensul său mai restrâns, diplomația publică încearcă să creeze un mediu politic și social sănătos în rândul opiniei publice străine, care să fie favorabilă și chiar deschisă eventualelor propuneri politice atunci când și dacă acestea sunt prezentate în contextul potrivit. În acest sens, se pregătește terenul pentru mai multă diplomație directă și de calitate. În sensul său mai larg, diplomația publică servește aproape ca o nouă paradigmă diplomatică, în care diplomații încearcă să faciliteze interacțiunile și conversațiile între grupurile societății civile pentru a ajuta la abordarea problemelor globale ale Noii Agende Internaționale de Securitate. Modalitatea nefastă de practicare a diplomației publice de către guverne se referă la ceva mai mult decât la propagandă și marketing, aceasta încercând să găsească o măsură marginală mai subtilă de a livra măsuri politice. În acest context de practicare a unor măsuri anti-diplomatice, putem

aduce în prim plan o previziune bazată pe date statistice „din teren" a unor furnizori de soluții de securitate chiar și în sectorul guvernamental, unde se așteaptă pentru perioada imediat următoare un val de „*imixtiuni în alegerile din Europa, unde anul alegerilor europarlamentare va atrage interes deosebit pentru atacuri informatice sponsorizate de entități statale asupra sistemelor de votare, dar și pentru propagandă pe rețelele de socializare și alte forme de imixtiune. Considerate altădată scenarii conspiraționiste, evenimentele din ultimii doi ani (2017-2018) arată că guvernele străine ar face orice ca să influențeze rezultatele alegerilor din țări unde au interese strategice*".[1] Urmare a acestor prognoze, în cursul lunii februarie 2019, Microsoft a relatat pe pagina oficială faptul că hackerii din gruparea rusă Strontium, cunoscută și sub numele de Fancy Bear și APT28, fiind de asemenea afiliați serviciului de informații militar rus sau GRU, au trimis e-mailuri de phishing către angajații care lucrează la monitorizarea alegerilor și urmărirea campaniilor de dezinformare politică din cadrul Fondului German Marshall, Institutului Aspen și Consiliul German pentru Relații Externe, având ca scop primar înșelarea țintelor și motivarea acestora în a accesa link-uri prin care ajungeau să-și piardă date și informații sensibile. Au fost identificate 104 atacuri asupra adreselor de e-mail din Belgia, Franța, Germania, Polonia, România și Serbia[2].

În ceea ce privește abordarea parteneriatului public-privat în România, aceste acțiuni progresiste deschid o nouă nișă prin care ONG-urile și grupurile societății civile pot lua inițiativa în ceea ce privește dezvoltarea în sine a noii paradigme. Diplomația digitală trebuie să scape de eticheta „obscură" avută în acest moment în zona cibernetică și să își cultive o cultură proprie, cu un rol bine stabilit și

1. Bitdefender, „Zece predicții despre atacurile cibernetice din 2019", 10.12.2018, https://www.bitdefender.ro/news/zece-predic%EF%BF%BD%EF%BF%BDii-despre-atacurile-cibernetice-din-2019-3607.html, accesat în data de 07.03.2019.
2. Tom Burt, „New steps to protect Europe from continued cyber threats", 20.02.2019, https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/, accesat în data de 07.03.2019.

echilibrat în știința sau arta diplomației. Diplomația digitală trebuie să se concentreze asupra domeniilor în care poate sprijini strategiile diplomatice mai largi - diplomația publică, crearea de rețele, colectarea informațiilor și gestionarea cunoștințelor, rezolvarea conflictelor și medierea - și asupra evoluției tehnologiilor și a platformelor și instrumentelor online care pot oferi cele mai eficiente rezultate. Mijloacele sociale existente vor continua să joace un rol important atunci când vor fi folosite inovator și creativ, însă actorii diplomatici nu ar trebui să depindă de ele. Mai degrabă ar trebui acum să lucreze împreună cu designerii de software pentru a dezvolta platforme personalizate, concepute special pentru a satisface nevoile diplomației secolului XXI. Acestea vor include platforme online care vor promova utilizarea mai intensă a tehnicilor de construire a scenariilor, de simulare și de adaptare a activităților din mediul online (jocuri, manuale interactive șamd.). Aceste instrumente noi din arsenalul diplomației digitale vor cântări mult în favoarea organizațiilor non guvernamentale și a altor grupuri și comunități ale societății civile.

În plan european, România se evidențiază printr-o participare diplomatică pro-activă la reglementarea spațiului cibernetic, precum în cazul Comisiei pentru Ocuparea Forței de Muncă și Afaceri Sociale și în cadrul Comisiei pentru Libertăți Civile, Justiție și Afaceri Interne din Parlamentul European, unde reprezentanți diplomatici români și membri ai Parlamentului European au fost desemnați ca raportori ai diferitelor grupuri politice pentru dosarul privind Piața Unică Digitală. Actul *„Piața Unică Digitală"* este un document foarte tehnic, iar dată fiind competența Comisiei, în cadrul acesteia au fost cooptați membrii care și-au adus contribuția concentrată pe subiectul combaterii conținutului ilegal în orice formă pe internet, dar și asupra protecției datelor cu caracter personal. Cu această ocazie s-a cerut opinia prin forme de consultanță *„pro bono"* din partea unor specialiști în domeniu. Din acest grup de lucru am făcut parte și eu

și am contribuit cu informații relevante și deosebit de utile cu privire la raportul Piața Unică Digitală Europeană.

Un alt exemplu al bunei diplomații românești în plan internațional, al cărui rezultat are implicații majore asupra relațiilor internaționale și de securitate la care România este asumată, este Summitul[1] NATO[2] 2018, organizat la Bruxelles în perioada 11-12 iulie 2018. În Declarația oficială emisă în urma Summitului este recunoscută influența instabilității securității cibernetice prin factorii de risc și amenințările vădit existente la adresa întregii alianțe, ceea ce ridică ștafeta la un nou nivel de abordare diplomatică. Noile provocări pe toate liniile strategice ale NATO (actori statali, actori non-statali, forțe militare, atacuri teroriste, cibernetice și hibride) îngreunează procesul diplomatic, acesta devenind unul complex prin natura sa mixtă. Mulți alți factori decisivi conturează aspectul formei de diplomație la nivelul național (românesc), european, internațional și global. Printre aceștia se numără și provocările hibride, incluzând aici campaniile de dezinformare și activități cibernetice malițioase.[3]

Cunoscându-se diferența de abordare cu privire la spirala de securitate cibernetică și paradigma diplomației securității cibernetice la nivelul UE, respectiv la nivel NATO, găsesc un punct comun, bine fundamentat de nevoile stringente din perspectiva relațiilor internaționale. Adânc fundamentată în amenințările aduse la securitatea uniunii și alianței (care este din ce în ce mai fragilă), tot mai frecvente, complexe, distructive și coercitive, tratate printr-o politică diplomatică persuasivă bazată pe putere militară și adesea economică, statele aliate sunt în poziția în care sunt nevoite să își asume un set nou de reguli, politici și proceduri. Cu alte cuvinte, un model

1. SUMMIT, summituri, s. n. Întâlnire (politică) la cel mai înalt nivel a unor șefi de stat. [Pr.: sámit] – Din engl. summit, DEX ,09 (2009).
2. NATO: Organizația Tratatului Atlanticului de Nord.
3. „Brussels Summit Declaration", Press Release (2018) 074 Emis în 11.07.2018, Punctul nr.2, https://www.nato.int/cps/en/natohq/official_texts_156624.htm, accesat în data de 14.07.2018.

unic de diplomație modern europeană trebuie teoretizat în cel mai scurt timp. Această nouă formă de diplomație, de departe diferită de diplomația tradițională bazată pe relații interumane, este una bazată pe gestionarea puterii și securității informației în sectorul cibernetic în egală măsură cu capacitatea întregii uniuni, alianțe și națiuni de a-și păstra și proteja valorile fundamentale.

În această ordine de idei, NATO a luat atitudine față de provocările aduse de sectorul cibernetic și a început încă din 2016 o serioasă campanie de operaționalizare a spațiului cibernetic pe întreaga circumscripție a alianței. Funcțiile operaționale de apărare în mediul cibernetic au determinat alianța să inițieze un set de exerciții, precum exercițiul *Cyber Endeavor,* care a urmat imediat după exercițiul militar declanșat de NATO *Trident Juncture 18*, cel mai amplu din ultimii ani, și pregătiri în acest domeniu.[1]

1. Lillian Ablon, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, Julia A. Thompson, PE-329-NATO, *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*, Edit. RAND Corporation, Santa Monica, USA, 2019, pp.8-13.

Capitolul V.
Influențe ale unei politici unitare europene privind securitatea informației electronice în actuala stare geopolitică globală

V.1. Abordarea de politică externă a României

România aduce în prim plan, prin expunerea oficială a Ministerului Afacerilor Externe, un comunicat prin care afirmă că oficial s-a luat atitudine privind noile trenduri prin adoptarea Strategiei de securitate cibernetică a României[1] și acțiunile MAE în privința securității cibernetice la nivel național, iar internațional prin existența Directi-

1. Securitate cibernetică, „Strategia de securitate cibernetică a României", https://www.mae.ro/node/28367, accesat astăzi 07.03.2018.

velor Uniunii Europene, precum Directiva[1] 2016/1148 *privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune* (intrată în vigoare în august 2016).

Ministerul Afacerilor Externe își aduce contribuția la regularizarea sistemului informațional din punct de vedere diplomatic prin calitatea de componentă a SNSC[2] şi de membru permanent în cadrul Consiliului Operativ de Securitate Cibernetică/COSC şi al Grupului de Suport Tehnic/GST.

Viziunea Ministerului Afacerilor Externe este una lăudabilă, cu atât mai mult cu cât reprezintă interfața de comunicare între structurile diplomatice şi consulare ale României din Serviciul Extern. MAE este prezent în procesul de comunicare și soluționare alături de autoritățile şi instituțiile naționale cu atribuții în continuitatea și operativitatea sistemelor de securitate cibernetică la nivel național. La baza acestei inițiative stau *Documentul Sinteză privind Politicile și Programele Bugetare pe termen mediu ale Ordonatorilor Principali de Credite pentru anul 2018 și perspectiva 2019-2021*, care aduc, conform priorităților strategice, pe termen mediu, o viziune laudativă de transformarea digitală a MAE.

Printre aceste proiecte, se numără:

A. *„implementarea „Strategiei MAE pentru o diplomație digitală", prin identificarea surselor potențiale de finanțare, atât bugetare, cât și externe, pentru implementarea strategiei, finalizarea listei de proiecte asociate și elaborarea unei scheme de finanțare a acestora,*

1. Directiva Europeană: *„Directivele le solicită statelor membre să obțină un anumit rezultat, fără a impune însă și modalitățile prin care pot face acest lucru. Statele membre trebuie să adopte măsuri prin care să încorporeze directivele în legislația națională (transpunere) în scopul de a atinge obiectivele stabilite de acestea. Autoritățile naționale trebuie să comunice Comisiei Europene aceste măsuri. Transpunerea în legislația națională trebuie să aibă loc înainte de termenul stabilit în momentul adoptării unei directive (în general în termen de 2 ani). Atunci când o țară nu transpune o directivă, Comisia poate iniția o acțiune în constatarea neîndeplinirii obligațiilor."*
2. SNSC: Sistemul Naţional de Securitate Cibernetică.

analizarea opțiunilor de realizare a unui proiect strategic pentru elaborarea arhitecturii organizaționale a MAE;

B. *dezvoltarea rețelelor de comunicații și creșterea siguranței cibernetice, prin:*
   - □ *reorganizarea și optimizarea rețelelor centralei MAE, introducerea accesului la mail de pe dispozitivele mobile;*
   - □ *finalizarea procedurii de răspuns rapid la incidente cibernetice, împreună cu SIE și Centrul Național Cyberint/SRI;*

C. *continuarea implementării/administrarea sistemelor existente și a proiectelor conexe:*
   - □ *sistemul național de informații privind vizele SNIV;*
   - □ *înființarea SPoC (Single Point of Contact) și adaptarea în vederea acordării accesului la sistemul central Schengen;*
   - □ *sistemul informatic pentru managementul integrat al serviciilor pentru cetățeni (SIMISC);*
   - □ *sistemul național de gestiune și emitere a pașapoartelor electronice ePASS;*
   - □ *participarea la proiectul de gestiune și emitere a cărții de identitate;*
   - □ *rezolvarea problemei mentenanței la sistemele informatice importante;*
   - □ *elaborarea unei noi versiuni a familiei de site-uri MAE, inclusiv pentru dispozitive mobile;*
   - □ *integrare cu site-ul web al Guvernului și cu portalurile consulare;*

Într-o egală măsură, se asigură un deosebit interes administrării și modernizării sistemelor informatice și de comunicații prin care sunt gestionate informații naționale, NATO și UE clasificate între Centrala MAE-Serviciul exterior și instituțiile din cadrul administrației centrale.

- *revizuirea măsurilor de securitate instituite în Centrala MAE și Serviciul exterior pentru prevenirea acțiunilor teroriste (dotarea*

cu echipamente de detectare și control și elaborarea de proceduri de lucru);

- *realizarea și administrarea unui sistem informatic și de comunicații prin care să fie gestionate informațiile neclasificate dar sensibile aferente problematicii UE, care să asigure conectarea Centralei MAE cu Reprezentanța Permanentă a României la Bruxelles și ministerele de linie;*
- *extinderea și acreditarea deplină de securitate a sistemului informatic și de comunicații clasificat EXTRANET Ro prin care MAE este conectat cu autorități și agenții ale administrației centrale;*
- *operaționalizarea și acreditarea unui sistem informatic și de comunicații clasificat cu nivel de secretizare SECRET UE prin care să fie gestionate informații UE clasificate între Centrala MAE (Registrul Intern UE și Reprezentanța Permanentă a României la Bruxelles - Registrul Extern UE);*
- *testarea, în cadrul Centralei MAE, a proiectului pilot al Registrului electronic pentru evidența corespondenței neclasificate;*
- *probleme în atenție în domeniul securității cibernetice:*
    - □ *consolidarea unei politici diplomatice cibernetice coerente și cuprinzătoare, conformă cu recomandările UE din cadrul Strategiei Globale a UE pentru Politica Externă și de Securitate;*
    - □ *participarea MAE la "Transpunerea și aplicarea Directivei NIS a UE" (Directiva UE 1148/2016 privind măsuri pentru un nivel ridicat comun de securitate a rețelelor și a sistemelor informatice în Uniune);*
    - □ *participarea MAE în cadrul Grupului de Lucru pentru Securitate Cibernetică la nivel UE;*
    - □ *responsabilități care decurg din participarea MAE în cadrul Consiliului Operativ pentru Securitate Cibernetică;*
    - □ *participarea în cadrul Comitetului de Coordonare a primului exercițiu de securitate cibernetică desfășurat la nivel național (CyDEx) pentru testarea capacității instituțiilor cu atribuții*

în domeniul securității cibernetice de a apăra Infrastructurile Critice de Importanță Națională;

- *implementarea deciziei Summit-ului NATO de la Varșovia privind recunoașterea spațiului cibernetic ca domeniu operațional;*
- *îndeplinirea angajamentului de consolidare a apărării cibernetice la nivel național ("Cyber Defence Pledge") - autoevaluarea nivelului de maturitate a capabilități de apărare cibernetică la nivel național;*
- *continuarea dialogului MAE-Ambasada SUA în cadrul Grupului de Lucru pentru securitate cibernetică România-SUA, pentru evaluarea posibilității realizării de proiecte bilaterale în cadrul oferit de "Cadrul pentru Securitate Cibernetică" (Cybersecurity Framework - CSF) al SUA, cum ar fi cel al dezvoltării unui "oraș inteligent" în România;*
- *coordonarea implementării de către instituțiile cu responsabilități în domeniu a setului de măsuri OSCE pentru creșterea nivelului de încredere în securitatea cibernetică (CBMs).*[1]

Conform sectorului de responsabilitate al Ministerului Afacerilor Externe, acestuia îi sunt atribuite și roluri de reprezentare activă la nivel național în cadrul inițiativelor organizațiilor internaționale în care este angrenat. Activitatea acestuia este necesară și în domeniul definirii măsurilor de creștere a încrederii și capacitării resurselor la nivel internațional privind utilizarea și normarea spațiului cibernetic. Așadar, MAE are rolul de a promova proactiv interesele naționale în domeniul securității cibernetice în orice context prielnic și în orice format de parteneriat sau cooperare internațională în care România este prezentă şi susține pro-activ dezvoltarea cooperării și parteneriatelor strategice și operaționale la nivel internațional, în vederea

1. Ministerul Afacerilor Externe, „Document sinteză privind politicile si programele bugetare pe termen mediu ale ordonatorilor principali de credite pentru anul 2018 si perspectiva 2019-2021", pp.18-19, http://www.cdep.ro/pdfs/buget/2018/anexa3/Ministerul%20Afacerilor%20Externe.pdf, accesat în data de 04.03.2019.

îmbunătățirii capacității de răspuns în cazul atacurilor cibernetice majore, care nu mai sunt de multă vreme un mit.

MAE este în egală măsură și instrumentul sau instituția care îndeplinește funcția de livrare a informațiilor de interes național către autoritățile şi instituțiile naționale românești și de informare privind modalitatea de îmbunătățire și dezvoltare în vederea obținerii unor rezultate competitive pentru mecanismele naționale românești de securitate cibernetică, cu impact la nivel regional sau internațional, cu raportare directă la UE, NATO, OSCE, CE.

„În cadrul organismelor de decizie şi execuție, create în scopul operaționalizării SNSC, respectiv în cadrul COSC şi GST, MAE a participat la întocmirea „Planului de acțiune la nivel național privind implementarea" SNSC şi a stabilit, împreună cu reprezentanții instituțiilor care alcătuiesc SNSC, liniile de acțiune şi sarcinile care revin ministerului potrivit domeniului de responsabilitate. Astfel, potrivit sarcinilor care derivă din Planul de acțiune privind implementarea SNSC, MAE a îndeplinit următoarele activități:

- √ *a constituit o bază de date cu privire la parteneriatele strategice - acorduri şi convenții - unde România deține calitatea de partener în domeniul securității cibernetice (NATO, UE, non-NATO şi non-UE);*
- √ *a pus la dispoziția COSC documentarul cu privire la abordarea securității cibernetice la nivelul organizațiilor internaționale şi reprezentarea naţională în cadrul acestora;*
- √ *a creat în cadrul Centralei MAE şi a Serviciului extern, un mecanism de informare reciprocă cu privire la preocupările la nivel internațional pe problematica securității cibernetice;*
- √ *asigură informarea membrilor GST cu privire la evoluțiile în domeniu semnalate de către reprezentanțele diplomatice şi consulare din Serviciul extern."*[1]

1. MAE, „Rolul MAE în privinţa securităţii cibernetice la nivel naţional", https://www.mae.ro/node/28366, accesat în data de 04.07.2018.

V.1.1. Contextul securității prin reziliență cibernetică

Dacă dorim să definim teoretic reziliența cibernetică, o putem descrie ca *abilitatea de a furniza continuu rezultatul dorit, în ciuda evenimentelor cibernetice adverse*.

Această *abilitate* poate fi luată în considerare la diferite nivele, conform Tabelului nr.6[1], unde fiecare nivel aduce provocări, metode și tipuri de controale conceptuale unice în raport cu reziliența cibernetică. Prin urmare, capacitatea de a furniza în mod *continuu rezultatul dorit* se referă nu numai la o națiune, ci și la o organizație sau chiar la un sistem IT specific. Cu toate acestea, pentru ca reziliența cibernetică să fie eficientă, aceasta trebuie abordată în modalitate holistică pe mai multe nivele și în paralel.

Nivel	**Descriere**	**Exemplu**
Supranațional	Reziliență cibernetică pentru o confederație de națiuni	Uniunea Europeană
Național	Reziliență cibernetică pentru o societate sau țară	România
Regional	Reziliență cibernetică pentru o regiune sau un oraș	Oradea
Organizațional	Reziliență cibernetică pentru o organizație	Companie, agenție, consiliu
Funcțional	Reziliență cibernetică pentru un element din sectorul de afaceri	Divizie, proces, capabilitate
Tehnic	Reziliență cibernetică pentru un sistem tehnologic	Sistem IT&C, rețea

Tabelul nr.6. Reziliența cibernetică expusă pe șase nivele

Termenul *continuu* contextual reprezintă abilitatea sau capacitatea de a furniza rezultatul dorit chiar și în momentul în care sistemele sau mecanismele uzuale, în urma unei breșe de securitate sau a unei situații neprevăzute, cedează sau sunt în incapacitatea de a furniza rezultatul scontat. Noțiunea *continuu* face referire și la abilitatea de a restaura, soluționa, repara și de a modifica sau schimba mecanismele

1 Deborah J. Bodeau, Richard Graubart, „Cyber Resiliency Engineering Framework", în *MITRE Tehnical Report (2011)*, Bedford, Massachusetts, 2011, p.37.

de furnizare a rezultatelor scontate care au dat greș și de a asigura continuitatea proceselor bazate pe analize de risc și prognoze.

Rezultatul dorit se referă în acest caz la rezultatul propus de către unitatea de analiză - statul, organizația sau sistemele IT&C - rezultate propuse precum obiective de afaceri, procese de continuitate a afacerii, servicii livrate în urma soluțiilor online și multe altele.

Evenimentele cibernetice adverse pot fi rezultatul a două tipuri generale de cauze, anume cele de sub incidența factorilor naturali și cele de sub incidența factorilor umani, precum sunt identificați în tabelul nr. 7.

Tipul de eveniment	**Descriere**	**Mod**	**Exemple**
Natural	Evenimente cauzate de natură	Necondiționat	Inundații, cutremure, tsunami, trăsnete, incendii șamd.
Uman	Evenimente cauzate de factorul uman	Intenționat	Acțiuni provocate din interiorul sau exteriorul organizației care pot afecta sistemele, rețelele, aplicațiile, datele informatice sau utilizatorii; **Fizice:** furt, deteriorare, reconfigurare **Electronice:** infracțiuni informatice.
		Neintenționat	**Interne:** operare incorectă, închidere accidentală, supraîncărcare ale unor servicii șamd.; **Externe:** defectul din fabricație, întreruperea unui serviciu șamd.

Tabelul nr.7. Evenimentele cibernetice adverse

Analizând literatura de specialitate, am considerat potrivită expunerea într-un studiu comparativ a rezilienței cibernetice și a securității cibernetice care sunt corelate desigur, dar nu neapărat interdependente. Cu toate că unele elemente pot părea comune sau

chiar aceleași, am identificat un număr de cinci caracteristici esențiale ale rezilienței cibernetice care au fost examinate și analizate în raport cu diferențele caracteristicilor esențiale ale securității cibernetice.

Caracteristică	**Securitate cibernetică**	**Reziliență Cibernetică**
Obiectiv	Protejarea sistemelor IT&C	Asigurarea livrării serviciilor
Intenție	Asigurarea rezistenței sistemului	Întrerupere controlată
Abordare	Asigurarea securității din mediul extern	Asigurarea securității din mediul intern
Arhitectură	Protecție pe un singur nivel	Protecție prin mai multe nivele
Scop	Atomistic[1], o organizație	Holistică[2], rețea de organizații

Tabelul nr.8. Caracteristicile securității cibernetice în raport cu reziliența cibernetică

Deși obiectivul principal al securității cibernetice stă în protejarea rețelelor de comunicații și tehnologia informației, respectiv a sistemelor informaționale, conform tabelului de mai sus și a analizelor de fapt, reziliența cibernetică este orientată mai degrabă spre asigurarea livrării serviciilor indiferent de impedimentele apărute. Abilitatea de a furniza continuu rezultatul dorit din definiția rezilienței este transpusă într-o altă formă în procesul de livrare a serviciilor afacerii ca obiectiv principal al organizației. Astfel, se confirmă capacitatea unui sistem cibernetic de a fi rezilient la un atac în momentul când, în ciuda evenimentelor de (in)securitate cibernetică, acesta își atinge obiectivul propus, chiar și prin utilizarea unor resurse alternative, uneori chiar identificate spontan conform contextului și situației de fapt. Desigur, ținem cont de faptul că implementarea unui sistem de reziliență cibernetică se face bazat pe nevoile și capacitățile afacerii propriu zise și croit pe obiectivele propuse de organizație și nu în aceeași măsură pe analizarea și asigurarea funcționalității sistemelor informatice și de comunicații. Cu alte cuvinte, necondiționat, reziliența cibernetică trebuie să fie în măsură să mențină sau să readucă în operativitate sectoarele care asigură furnizarea de produse ori servicii.

1. John P. Miller, „Atomism, Pragmatism, Holism", în *Journal of Curriculum and Supervision*, Vol.1, nr.3, 1986, pp.175-178, http://www.ascd.org/ASCD/pdf/journals/jcs/jcs_1986spring_miller.pdf, accesat în data de 20.02.2019.
2. *Ibidem*, pp.183-189.

Pentru a oferi un rezultat bazat pe caracteristicile securității cibernetice, intenția în raport cu obiectivele de mai sus, conform tabelului nr. 5, trebuie să îndeplinească nevoile constructive ale sistemului sau ale sistemelor. Intențiile securității cibernetice sunt de a gestiona prin construcție și de a proteja sistemul pentru a furniza continuu, chiar și în momente de criză, un comportament de rezistență și neîntrerupere a serviciilor și furnizării produselor, asigurat de măsuri riguroase de securitate. În contrast cu intenția securității cibernetice, caracteristicile rezilienței cibernetice sunt de a asigura o întrerupere controlată și sigură a sistemului ori sistemelor în cazul unui eveniment cibernetic.

Al treilea aspect definitoriu al rezilienței cibernetice este abordarea generală a acesteia asupra sistemului. Din perspectiva securității cibernetice, protejarea proceselor prin elemente de securizare independente de sistemul de securitate propriu este ceva acceptat, pe când, din perspectiva securității prin reziliență cibernetică abordarea este ceva mai profundă. În cazul securității bazate pe reziliență, accentul se pune mereu pe adoptarea și implementarea unui sistem de securitate complet. Ne referim aici la soluții complexe care să conțină ele însele elementele și servicii externalizate în cazul securității cibernetice, cum este cazul subsistemelor ce alcătuiesc organizația ori a sistemelor de comunicații și tehnologia informației. Identificăm așadar necesitatea utilizării mai multor tehnici reactive, cum ar fi operațiunile alternative și compoziția dinamică a caracteristicilor atunci când se construiesc sisteme de securitate reziliente.

Arhitectura unui sistem, fie acela de securitate sau reziliență cibernetică, trebuie să fie dinamică. Cu toate că din perspectiva teoretică a securității cibernetice, nu este acceptat eșecul prin apariția breșelor de securitate sau a evenimentelor de securitate, riscurile sunt cu atât mai mari pentru continuitatea serviciilor cu cât lipsa de flexibilitate a sistemului la atacuri sau incidente este mai scăzută. Astfel, rigiditatea unui astfel de sistem nu atenuează și nici nu scade impactul unei

întreruperi a sistemului pentru livrarea serviciilor care se consideră că trebuie să fie furnizate într-un sistem continuu. Conceptul cu care se lucrează în construirea unei arhitecturi de securitate cibernetică rezilientă este de a utiliza cât mai multe niveluri de securitate cu nivel mic de incidență în caz de întrerupere a serviciilor și sistem propriu de protecție și reziliență pe fiecare nivel în parte. În general, sistemele de securitate cibernetică reziliente sunt adoptate mai greu de rețelele în care se vehiculează informații clasificate secrete de stat, tocmai din cauza acestei permisivități și flexibilități la incident[1].

Cu siguranță scopul unei soluții de reziliență cibernetică nu este de a menține funcționalitatea unui singur sistem sau organizații cu elementele imediat tangențial-conectate. Motivația alegerii și implementării unui astfel de sistem este dată de nevoia de analiză continuă a stării de fapt a întregului sistem față de toate sectoarele care sunt pasibile de a aduce o stare de vulnerabilitate, precum și de nevoia de asigura continuitatea afacerii și a furnizării serviciilor ori produselor propuse, prin asigurarea unei reziliențe a tuturor sub-sistemelor, care însumate duc la buna funcționare a sistemului primar pentru care se proiectează sistemul de reziliență cibernetică- servicii externe, furnizori de produse și echipamente șamd. Un management rezilient în contextul securității cibernetice cuprinde separat segmentul organizațional față de cel al sistemelor IT&C care să fie analizate în contextul unei rețele interdependente.

Cu toate că interesul față de literatura de specialitate în acest moment este unul crescut și urmează un trend ascendent în ultimii douăzeci de ani, totuși odată cu aceasta abordare a problematicilor în care securitatea este factor decisiv - precum reziliența cibernetică a organizațiilor sau a statelor - primele studii de securitate cu rezonanță și aplicabilitate în sectorul politic au apărut din segmentul cercetărilor

1. Patricia A H Williams, Rachel J. Manheke, „Small Business-A Cyber Resilience Vulnerability", în *Proceedings of the 1st International Cyber Resilience Conference,* Edit. Cowan University Research Online, Perth Western, 2010, pp.113-115.

teoriilor politice convenționale sau clasice, care sunt atent abordate în ultima decadă[1].

Siguranța cibernetică transcende înțelegerea convențională a literaturii de specialitate în domeniul securității naționale în raport cu relațiile internaționale. Dilema de securitate în acest caz este provocată în mod direct de caracterul transfrontalier al infracțiunilor informatice și de nevoia cooperării statelor prin organismele sale specializate din spectrul internațional. Pentru a veni în ajutorul acestor organisme, de regulă, se solicită expertiza de specialitate din sectorul securității cibernetice și din partea actorilor non statali, din sectorul privat. Orientându-ne atenția spre tipologia atacurilor cibernetice, putem observa că primul răspuns la astfel de atacuri vine din partea țintei sau victimei. Prin urmare, sectorul general de securitate s-a privatizat în toată lumea, rămânând privată de ochii actorilor non statali doar securitatea națională. În anii 1990, infrastructurile critice au devenit principalul subiect al dezbaterilor din zona relațiilor internaționale privind securitatea cibernetică. Protecția infrastructurilor critice cuprinde mai mult decât securitatea cibernetică, însă aspectele cibernetice au fost principalul motor al acestor noi seturi de politici care au ajuns la un moment dat chiar politici de referință[2], aplicate în unanimitate de SUA și mai nou de anumite state ale UE. Particularizând, sugerez o privire de detaliu la abordarea securității cibernetice în prezent de către actorii non statali. Observăm aici o certă dezvoltarea a soluțiilor de securitate, precum

1. Alexander Klimburg, Hugo Zylberberg, „Cyber Security Capacity Building: Developing Access”, în *NUPI Report nr.6*, Edit. Norwegian Institute of International Affairs, Oslo, 2015, p.23; Fredrik Björck, Martin Henkel, Janis Stirna, Jelena Zdravkovic, „Cyber Resilience - Fundamentals for a Definition”, în *New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing*, Vol.353, Edit. Springer, Cham, 2015, p.313; George Christou, *Cybersecurity in the European Union - Resilience and Adaptability in Governance Policy*, Edit. Palgrave Macmillan, 2016, pp.11-12.
2. Myriam Dunn Cavelty, „Cybersecurity in Switzerland”, în *Springer Briefs in Cybersecurity*, Edit. Springer International Publishing, Zürich, 2014, p.18.

programele sau platformele antivirus din ce în ce mai complexe - cu soluții de echipamente fizice și cloud șamd., dar și a unor companii care se ocupă cu soluții unice, adaptate la nevoile organizațiilor - chiar și din sectorul public - la un nivel profesional pe care statele prin forțele lor proprii și limitele de dezvoltare - inovare nu le-ar fi putut atinge într-un timp atât de scurt. Drept urmare, expertiza în securitate cibernetică a actorilor privați a fost cea la care s-a apelat de fiecare dată când era nevoie de o soluție eficientă și agreată atât de adepții guvernanței convenționale, cât și de cei ai cele nonconvenționale sau nesupuse rigorilor ierarhice. Ca urmare a acestei nevoi, care a ajuns chiar la o formă de interdependență într-o formă mai elaborată și dezvoltată, s-au format parteneriate public-private, care sunt și azi menite să faciliteze și să protejeze serviciile critice, cum ar fi serviciile de telecomunicații sau serviciile bancare, servicii care sunt vitale funcționării statului. În domeniul securității cibernetice, aceste parteneriate sunt gestionate prin intermediul instituțiilor cu activitate de nișă apărute în urma revoluției tehnologice și politice în sectorul securității cibernetice în UE.

Luând în considerare faptul că în centrul mecanismului de răspuns la atac cibernetic stau, în următoarea ordine, organizațiile de profil din sectorul privat, persoanele afectate[1], organismele statului, iar persoanele sau utilizatorii resurselor din mediul virtual reprezintă cea mai mare vulnerabilitate[23], tot aceștia, utilizatorii, sunt și factorul de decizie cel mai important. Din perspectiva managementului elitist al sectorului cibernetic, ne punem întrebarea „Care este rolul actorului politic în guvernanța cibernetică a UE?”, întrebare la care, în contextul Uniunii Europene, putem răspunde dintr-o singură perspectivă, cea economică. Dacă vulnerabilitatea stă în capacitatea utilizatorului

1. Fredrik Björck, Martin Henkel, Janis Stirna, Jelena Zdravkovic, *op. cit*, p.313.
2. Alexander Klimburg, Hugo Zylberberg, *op.cit*, p.22.
3. William Arthur Conklin, Dan Shoemaker, „Cyber-Resilience: Seven Steps for Institutional Survival”, în *The EDP Audit, Control, and Security Newsletter*, Vol.55, Nr. 2, Edit. Taylor & Francis Group, 2017, pp. 14-22.

final de a se proteja sau de a-și securiza prezența online, capacitatea de securizare generală sau specifică stă în capacitarea cu elemente de securitate a organizațiilor de stat sau a celor private în raport cu contextul criminogen, sau pur și simplu în raport cu contextul de (in)securitate din aria de activitate în care ambii - persoana și organizația - activează, după cum reiese și din raportul ENISA ETL 2018[1].

Pentru a prezenta o poziție obiectivă și reală a nivelului de reziliență cibernetică la nivelul Uniunii Europene în domeniul securității cibernetice și evaluarea eficacității normativelor relevante adoptate de aceasta, trebuie să răspundem la cinci întrebări privind cadrul normativ care reglementează reziliența cibernetică, rolul instituțiilor supranaționale ale UE, teoriile care explică cel mai bine reziliența cibernetică în UE, modalitățile prin care UE își crește nivelul de reziliență cibernetică și gradul de eficiență al măsurilor luate de UE în ceea ce privește reziliența cibernetică, comună (în contextul statelor membre) fără o guvernare supranațională.

V.2. Problematica securității cibernetice din perspectiva organismelor internaționale şi implicarea României ca membru al acestora

V.2.1. Uniunea Europeană - UE

Pentru a înțelege rolul UE în această dilemă de securitate globală, suntem nevoiți să cunoaștem în profunzime obiectivele Uniunii Europene prin promovarea păcii, susținerea valorilor europene și bunăstarea cetățenilor săi, asigurarea unei stări de independență și libertate, un sentiment colectiv de securitate și justiție care transcede jurisdicția

1. ENISA Threat Landscape Report 2018 – „15 Top Cyberthreats and Trends, ETL 2018", 2019, p.74, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, accesat în data de 20.02.2019.

frontierelor interne și asigurarea unei dezvoltări durabile bazate pe creșterea economică echilibrată și pe stabilitatea prețurilor, prin menținerea și crearea unei economii de piață sănătoase și competitive care să favorizeze cu ajutorul UE, prin politica de coeziune, o ocupare integrală a disponibilității din piață cu forță de muncă, precum și progresul social și protecția mediului, fără a exclude combaterea excluziunii sociale și discriminarea. UE nu întârzie să încurajeze progresul tehnic și științific pentru a consolida planul de coeziune economică regională, pentru împlinirea obiectivelor secundare de ordin social și teritorial, precum și pentru solidaritatea statelor membre partenere în Politica de coeziune în exercițiu și negreșit pentru încurajarea respectului față de diversitatea lingvistică și culturală a statelor și regiunilor partenere în acest front comun. Nu în ultimul rând, UE este pro-activă în abordarea și dezvoltarea unui proiect de uniune economică și monetară cu moneda unică euro €, chiar dacă încă acest lucru nu a fost propagat pe întreaga jurisdicție a UE.

Analizând fundamental valorile UE, observăm că, deși sunt interpretări diferite de la stat la stat, acestea sunt valori existente la nivelul tuturor statelor membre. Aceste valori sunt necesare într-o societate în care se dorește alinierea la toleranță fără ca aceasta să fie dusă în derizoriu, la un cadru de justiție comun și unitar aplicabil în toată jurisdicția UE fără limitări, la o solidaritate în crearea și menținerea unui front comun de tip federal și la combaterea discriminării în limitele impuse de statutul suveran. Acestea sunt oglindirea oarecum filosofică a modului de viață european, *în extenso*. Cele cinci mari principii ale UE (*demnitatea umană, libertatea, democrația, egalitatea, statul de drept și drepturile omului*) au incidențe reale și unice în realitatea de zi cu zi a cetățenilor statelor membre și totodată sunt aplicabile realității virtuale, iar mecanismele implementate în domeniul cibernetic trebuie să respecte în totalitate aceste principii. Zona de întrepătrundere și conexiune între realitate și spațiul virtual nu este

realitatea augmentată, ci aici este vorba de două arealuri distincte care au aceiași cetățeni în două forme distincte.

V.2.2. Organizația Tratatului Atlanticului de Nord - NATO

„Este un plan[1] *ambițios, concret și pragmatic. [...] Acesta definește un nivel comun de ambiție pentru Uniunea Europeană."* HRVP Federica Mogherini,14 noiembrie 2016.

În cazul României, România, securitatea națională nu poate fi protejată doar de mecanismele interne ale statului și organismele naționale. În contextul de securitate actual, în calitate de țară membră UE și în același timp sub umbrela NATO, suntem una dintre fericitele cazuri în care poziția geostrategică a țării ne aduce un atu prin asigurarea implicării UE și a NATO în întărirea mecanismului securității naționale din perspectiva militară și cibernetică.

Progresul tehnologic și creșterea amenințărilor provenite din arealul cibernetic au dus la adoptarea de către NATO a unui noului concept şi politici în domeniul apărării, cu precădere în domeniul apărării cibernetice și recunoașterea spațiului cibernetic ca domeniu operațional.

Summit-ului NATO din Țara Galilor - Marea Britanie, din septembrie 2014, reprezintă un punct de cotitură pentru întreg conceptul militar. Cu ocazia acestui eveniment, șefii de stat şi de guvern au susținut și revizuit atât Politica Întărită a NATO în domeniul Apărării Cibernetice (trad. *Enhanced NATO Policy on Cyber Defence*), cât şi Planul de Acțiune revizuit. Rezultatul acestui Summit a fost marcat de introducerea pe agenda comitetului a temei cooperării NATO cu industria de specialitate în scopul realizării și întăririi cadrului de cooperare NATO-industrie, prevăzut de noua politică.

Cu ocazia Summit-ului NATO de la Varșovia, din 8-9 iulie 2016, s-a reafirmat mandatul defensiv al NATO și s-a recunoscut oficial

1. EEAS, „Implementation Plan on Security and Defence", https://eeas.europa.eu/sites/eeas/files/implementation_plan_on_security_and_defence_2.pdf, accesat în data de 30.04.2019.

spațiul cibernetic drept al cincilea domeniu al războiului, sau al cincilea teatru de operațiuni militar, astfel încât ar putea răspunde cu arme convenționale în cazul unui atac cibernetic puternic. În acest nou areal militar, ce necesită o atenție de securitate, NATO trebuie să fie rezilient și în deplină capacitate de exercițiu militar în toate spațiile care sunt definite ca posibile teatre de operațiuni, respectiv în spațiu aerian, terestru, maritim, spațial și cibernetic. Un atac cibernetic asupra unuia dintre statele membre NATO ar activa articolul 5, drept urmare se va cere un răspuns al alianței.

Conceptul a fost expus mass-mediei de către secretarul general al NATO, Jens Stoltenberg, acesta afirmând într-un interviu acordat presei nemțești (Ziarului Bild), faptul că *„Un atac cibernetic sever poate fi clasificat ca un caz pentru alianță. Apoi, NATO poate și trebuie să reacționeze. Cât despre evaluarea gravității atacului, NATO intenționează să răspundă la orice atac direcționat asupra membrilor NATO, inclusiv un atac cibernetic care ar putea fi considerat un act de război și toate țările NATO se vor sprijini reciproc pentru apărarea cibernetică a infrastructurii lor"*.

NATO a făcut un prim pas pentru îmbunătățirea capacității de protejare și desfășurare a operațiunilor în aceste spații unde, prin respectarea suveranității statelor membre, se va păstra libertatea de acțiune și de decizie. Acesta a fost urmat de semnarea declarației comune NATO-UE de la Varșovia, din 8 iulie 2016, care a dat un nou impuls și o nouă substanță UE- Parteneriatul strategic al NATO, parteneriat semnat între Președintele Consiliului European și Președintele Comisiei Europene, împreună cu Secretarul General al Organizației Tratatului Atlanticului de Nord.

În contextul strategic contemporan, cu provocări fără precedent provenind din sud și est, cooperarea dintre Uniunea Europeană și Organizația Tratatului Atlanticului de Nord este esențială. Securitatea UE și NATO este interconectată, cu 22 de state membre ale UE care au și calitatea de aliați NATO, într-un front comun prin care pot mobiliza și capacita un instrumentar strategic și operațional vast cu

o capacitate și pe măsura provocărilor, dar prioritar pentru a spori securitatea cetățenilor lor.

Acest parteneriat[1] a subliniat șapte domenii concrete în care ar trebui consolidată cooperarea dintre cele două organizații:

1. Combaterea amenințărilor hibride;
2. Cooperare operațională, inclusiv pe mare și migrație;
3. Securitatea și apărarea cibernetică;
4. Capabilități de apărare;
5. Industria de apărare și cercetarea;
6. Exerciții;
7. Sprijinirea eforturilor de consolidare a capacităților partenerilor din est și sud.[2]

În virtutea acțiunilor NATO de descurajare și apărare, domeniul apărării în arealul cibernetic va fi parte integrată din planificarea operațională în contextul și cadrul operațional și operativ al NATO.

În ceea ce privește în mod direct apărarea cibernetică, din perspectiva parteneriatului UE-NATO, se consideră că amenințările și atacurile cibernetice devenite tot mai frecvente, complexe și cu efecte tot mai grave, iar Alianța se confruntă cu un mediu amenințător, sensibil și complicat, cu amenințări iminente în toate planurile de securitate a informației. În urma ultimelor evenimente din 2018, s-a constatat că aceste atacuri cibernetice au fost cuprinse în modelul războiului hibrid. Așadar, NATO și aliații săi se bazează pe o apărare cibernetică puternică și rezilientă pentru a îndeplini sarcinile principale ale Alianței de apărare colectivă, de gestionare a crizelor și de securitate cooperativă. În contextul creșterii amenințărilor cibernetice și atacurilor cu care se confruntă NATO, este imperios necesar ca aceasta să fie capabilă să-și protejeze și să își securizeze rețelele

1. EEAS, Bruxelles, 2018, „EU-NATO cooperation”, https://eeas.europa.eu/sites/eeas/files/eu-nato_cooperation_factsheet.pdf, accesat în data de 30.04.2019.
2. EEAS, Bruxelles, 22/11/2018 - 10:55, UNIQUE ID: 170616_1, „EU-NATO cooperation – Factsheet”, https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en, accesat în data de 30.04.2019.

și operațiunile din orice direcție sau atac, fie acesta și unul sofisticat de tip APT distribuit la nivel regional sau global.

Sunt de subliniat sarcinile cele mai importante ale NATO în raport cu apărarea cibernetică:

- Apărarea cibernetică face parte din pachetul de sarcini fundamentale a NATO pentru apărare colectivă.
- NATO, asemenea UE, a afirmat că legislația internațională se aplică în spațiul cibernetic.
- În contextul apărării cibernetice, principalul obiectiv al NATO este acela de a-și proteja rețele proprii -inclusiv operațiunile și misiunile- și de a spori reziliența cibernetică în cadrul Alianței.
- În iulie 2016, aliații au reafirmat mandatul defensiv al NATO și spațiul cibernetic, recunoscut ca areal de operațiuni militar în care NATO trebuie să fie un puternic generator de securitate militară, în egală măsură ca în spații precum cel aerian, terestru, maritim sau spațial.
- Aliații au făcut, de asemenea, un angajament de apărare cibernetică în iulie 2016 pentru a-și îmbunătăți apărarea cibernetică, considerând-o o problemă prioritară. De atunci, aproape toți aliații și-au îmbunătățit apărarea cibernetică.
- NATO își consolidează capacitățile pentru educația, formarea și exercițiile cibernetice.
- Aliații se angajează să sporească schimbul de informații și asistența reciprocă în prevenirea, atenuarea și recuperarea atacurilor cibernetice.
- Echipele de Reacție Cibernetică Rapidă ale NATO sunt în regim de așteptare pentru a asista aliații, 24 de ore pe zi, dacă sunt solicitate și aprobate.
- La summitul de la Bruxelles din 2018, aliații au convenit să înființeze un nou Centru de Operațiuni a spațiului Cibernetic, ca parte a structurii de comandă consolidată a NATO. Aceștia au convenit, de asemenea, că NATO poate să se folosească

de capacitățile naționale cibernetice pentru misiunile și operațiunile sale.

- NATO și Uniunea Europeană (UE) cooperează printr-o înțelegere tehnică privind apărarea cibernetică, semnată în februarie 2016. În lumina provocărilor comune, NATO și UE își întăresc cooperarea în domeniul apărării cibernetice, în special în domeniul schimbului de informații, instruire, cercetare și exerciții.
- NATO își intensifică cooperarea cu industria prin Parteneriatul Industriei Cibernetice a NATO.[1]

Summit-ului NATO de la Varșovia, din 2016, s-a materializat și prin înființarea Centrului de Excelență pentru Amenințări Hibride în Finlanda, care a fost stabilit de mai multe țări NATO și UE (SUA, Marea Britanie, Germania, Franța, Italia, Spania, Polonia, Suedia și țările baltice), precum și de oficiali ai UE și NATO. Motivată de fenomenul combaterii amenințărilor hibride, care este extrem de important, având în vedere poziția geostrategică într-o regiune cu o dinamică de securitate ridicată, România, în 14.11.2018, devine cel de-al 19 stat membru UE al Centrului European de Excelență pentru combaterea amenințărilor hibride (Hybrid CoE), care își desfășoară activitatea la Helsinki, în Finlanda[2]. La demersul NATO-UE se adaugă încă două instrumente de cooperare, menționate și anterior:

- Declarația comună de cooperare UE – NATO, adoptată în marja Summit-ului NATO de la Varșovia, iulie 2016, privind consolidarea cooperării practice în anumite domenii.

1. NATO, 16.07.2018, „Cyber defence”, https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat în data de 30.04.2019.
2. Robert Lupitu, „România a devenit al 19-lea stat membru al Centrului European de Excelență pentru combaterea amenințărilor hibride, cu sediul la Helsinki”, 15.11.2018, https://www.caleaeuropeana.ro/romania-a-devenit-al-19-lea-stat-membru-al-centrului-european-de-excelenta-pentru-combaterea-amenintarilor-hibride-cu-sediul-la-helsinki/, accesat în data de 30.04.2019.

- Acordul tehnic de cooperare NATO-UE în domeniul securității cibernetice, semnat la data de 10.01.2016, între NATO Computer Incident Response Capability (NCIRC) și Computer Emergency Response Team - European Union (CERT-EU).

Proiectul cu privire la domeniul comunicării strategice (StratCom) a Alianţei din perspectiva apărării cibernetice, ce are ca obiectiv evidențierea laturii defensive a acțiunii NATO în sectorul cibernetic, a fost emis de Centrul de Excelenţă NATO pentru Comunicații Strategice de la Riga, Letonia. În același document a fost menționată și nevoia de alinieres a acțiunilor aliate în domeniu cibernetic la prevederile dreptului internațional.

Secretarul General al NATO, alături de oficialii de rang înalt ai NATO şi UE, au susținut și apreciat pozitiv Cyber Defence Pledge[1] și operaționalizarea Directivei UE care privește securitatea rețelelor și a informațiilor. Între NATO și UE un pilon strategic important este cooperarea, o necesitate importantă în dezvoltarea și soluționarea paradigmei de securitate în sectorul internațional atât pentru gestionarea operațiilor, cât şi a crizelor. Totodată, trebuie menționată intenția României de a face demersuri pentru aderarea în calitate de stat sponsor la „*NATO Cooperative Cyber Defence Centre of Excellence*" (CCDCOE) sau Centrul de Excelenţă NATO Tallinn, care este un reper în domeniul securității cibernetice pe plan mondial.

Desigur, România, prin reprezentanța sa în calitate de stat membru UE și aliat NATO, a participat la numeroase exerciții și acțiuni, respectiv misiuni concertate de organismele internaționale, deși rolul său, de cele mai multe ori, a fost unul consultativ. Dintre documentele semnate de România cu privire la guvernanța domeniul cibernetic, amintim:

1. Stoltenberg Jens, Secretar General NATO, Discurs, „Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris)", 15.05.2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm, accesat în data de 30.04.2019.

- *„Memorandum de Înțelegere pentru cooperarea în domeniul securității cibernetice între Comitetul NATO de Management al Apărării Cibernetice şi Serviciul Român de Informații din 18.10.2011, actualizat sub forma noului Memorandum de Înțelegere între CDMB și SRI semnat la 23.06.2016, în conformitate cu Politica Întărită a NATO în domeniul apărării cibernetice;*
- *Memorandum de Înțelegere între Canada, Danemarca, Norvegia, Olanda, România şi Organizația NATO pentru Comunicații şi Cibernetică (NCIO) pentru participarea la proiectul Multinațional de Dezvoltare a unor Capabilități în domeniul apărării cibernetice*[1].

În aprilie 2016, Centrul Național Cyberint a organizat la București, cu sprijinul MAE, reuniunea de tip „Away Day" a Comitetului pentru Apărare Cibernetică al NATO, care a reunit la București toți reprezentanții delegațiilor permanente ale statelor aliate la NATO, ocazie cu care România a prezentat evoluțiile în domeniul securității cibernetice și al apărării cibernetice, inclusiv la nivel educațional și al capacităților în domeniu (vizita la Centrul Național Cyberint și la Centrul de Inovare pentru Securitate Cibernetică - proiect pilot lansat în 2015 cu sprijinul USAID și CERT-RO)"[2].

V.2.3. CONSILIUL EUROPEI - CoE

Consiliului Europei este organismul supranațional al UE printre obiectivele căruie să numără și gestionarea problematicii criminalității

1. *România participă, alături de Canada (lider de proiect), Danemarca, Norvegia, Olanda. Activitatea se va derula pe trei pachete de lucru, iar România coordonează unul dintre cele trei pachete de lucru. MNCD asigură schimbul de informaţii privind incidenţele cibernetice (inclusiv informaţii „malware"), între CSIRTs naţionale („Computer Security Incident Response Teams" – trad. „Echipele de Răspuns la Incidentele de Securitate Informatică"); creşterea gradului de conştientizare a situaţiei naţionale de apărare cibernetică, prin dezvoltarea de interfețe specifice de depozitare de informaţii şi de vizualizare; punerea în comun a resurselor naţionale pentru a investiga modurile de detectare a activităţilor rău intenţionate efectuate prin Atacuri Direcţionate Avansate / APT („Advanced Persistent Threats") şi pentru a facilita evaluarea atacurilor şi a daunelor pe care le-au cauzat*
2. MAE, „Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora", https://www.mae.ro/node/28369?page=6, accesat în data de 04.07.2018.

din sectorul cibernetic, protecției datelor personale, dar şi a guvernanței internetului, în raport cu atingerea statutului democratic al statului și al persoanei, în raport cu mențiunile Cartei Internaționale a Drepturilor Omului şi a statului de drept a statelor membre UE.

Convenția privind criminalitatea cibernetică de la Budapesta[1] este principalul instrument juridic de reglementare a internetului şi combatere a infracțiunilor din spațiul virtual. În această ordine de idei, din punct de vedere criminologic, CoE deține rolul de observator și raportor în procesul de monitorizare a gradului implementării de către statele membre a normativelor europene în domeniu.

În urma propunerii președintelui României, Traian Băsescu, din 2013, către Consiliul Europei, capitala României se bucură de atenția exclusivă a acțiunilor CoE prin înființarea la București a Oficiului Regional pentru Combaterea Criminalității Informatice (C-PROC). . C-PROC a reprezentat materializarea Memorandumului de Înțelegere, semnat, la 15 octombrie 2013, între Ministerul Afacerilor Externe a României şi Secretariatul General al Consiliului Europei de la Strasbourg.

Oficiul Regional pentru Combaterea Criminalității Informatice are ca obiectiv principal să analizeze criminologic situația infracțională din mediul cibernetic și să ajute în primul rând statele membre UE și alte state ale lumii să-și dezvolte capacități de contracarare a infracțiunilor cibernetice şi în domeniul probelor electronice în cazuri de infracțiuni de acest gen. Un aspect important îl are caracterul extern al C-PROC, acesta având atribuții de dezvoltare a capacităților împotriva atacurilor cibernetice în afara țării și chiar a UE.

Unul dintre motivele pentru care acest oficiu este prezent în România este dat de adoptarea legislației privind infracțiunile ciber-

1. Consiliul Europei, Details of Treaty No.185, „Convention on Cybercrime", https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accesat în data de 04.05.2019.

netice din 2004[1], care reprezintă un reper legislativ pentru celelalte state. Este unul dintre bunele exemple de aliniere a statelor membre UE prin adoptarea directivelor și emiterea în baza acestora de legi organice la nivel național, punctual și transparent, fără o reinterpretare a normativelor organismelor supranaționale. Acest exemplu este pentru țări din Europa, America Latină, Africa și Asia un model de urmat în contextul cooperării între magistrați și alte organisme cu rol judiciar. Provenind din mediul Ministerului Afacerilor Interne, pot confirma profunda implicare a judiciariștilor din unitățile de investigare a infracțiunilor cibernetice.

C-PROC de la București are, de asemenea, un rol activ în dezvoltarea capacității naționale/internaționale de combatere și contracarare a atacurilor cibernetice, inclusiv în cazul APT-urilor sau a intruziunii privind datele cu caracter personal.

Un studiu privind CoE ca instituție supranațională sau conferință interguvernamentală a arătat, în baza modelului de analiză multivariată, perspectiva generală a funcționării CoE, dar şi a caracteristicilor sale unice. În respectivul studiu s-a constatat, prin analiza variabilelor, faptul că o parte dintre acestea, (*Președinția CoE, Comitetul Reprezentanților Permanenți, ordinea de zi pe puncte A şi B, votul cu majoritate calificată, Secretariatul General al Consiliului, procedura de consultare şi de cooperare, dar şi procesul de socializare a elitelor*) se aliniază conceptului de construcție a entităților supranaționale a UE, în timp ce „*votul cu unanimitate*", „*procedura de codecizie*" şi „*Președinția CoE*" se asimilează caracteristic conferințelor interguvernamentale.

Un exemplu reprezentativ este dat de analiza Concluziilor CoE în urma întrunii CoE nr 2546 pe probleme de Afaceri Economice și Financiare de la Bruxelles, din 25 noiembrie 2003[2], unde decizia de

1. Parlamentul României, Legea nr. 64 din 24 martie 2004, *pentru ratificarea Conventiei Consiliului Europei privind criminalitatea informatică*, adoptată la Budapesta în 23 noiembrie 2001.
2. Comisia Europeană – CoE, „2546th Council meeting - Economic and Financial Affairs" - Brussels, 25 November 2003, http://europa.eu/rapid/press-release_PRES-03-

amânare a procedurii federale de deficit excesiv împotriva Republicii Federale Germania şi a Republicii Franceze arată că, deși CoE are capacitatea de exercițiu precum o instituție supranațională, în cazuri precum cel expus în cadrul întâlnirii mai sus menționate, paradoxal înțelegerii de uniune sau alianță regională, interesele statelor membre devin oarecum o prioritate și sunt probabil superioare intereselor instituțiilor și organizațiilor supranaționale. Motivația apare pe fondul nevoii de a se păstra în primul rând capacitatea de dezvoltare a procesului de integrare europeană și suveranitatea națională într-o uniune federală, deciziile luându-se într-o măsură echitabilă și în folosul statelor ca membre ale uniunii. Concluzia dată de evoluția Consiliul European și de acțiunile acestuia este că acesta reprezintă o instituție hibridă, o imixtiune de caracteristici specifice instituțiilor supranaționale, dar și specifice mecanismelor de relaționare interguvernamentală. Impactul CoE asupra procesului generic de integrare europeană este dat exclusiv și deloc exhaustiv de echilibrul dintre caracteristicile, atributelor, calităților și trăsături instituționale[1].

V.2.4. Organizația pentru Securitate și Cooperare în Europa - OSCE

Încă de la înființare (1970), OSCE joacă un rol important în consolidarea securității „*Noii Europe*" cu atât mai mult începând cu 2013, când OSCE acordă o atenție deosebită securității informatice (ICT). OSCE adoptă un set de măsuri în special pentru reducerea riscurilor de conflict dintre state care decurg din utilizarea TIC. O preocupare majoră în acest sens este dată de ONU prin grupurile de experți guvernamentali la nivel regional pe problematica securității cibernetice.

320_en.htm, accesat în data de 04.05.2019.

1. Alexandru Nicolae Clain, „Consiliul Europei - instituție supranațională sau conferință interguvernamentală?", în *Continuitate și schimbare în guvernanța europeană*, Vol. 4, Nr. 1, 2010, p.14, http://europolity.eu/wp-content/uploads/2014/05/Vol.4.1.-2010.pdf, accesat în data de 04.05.2019.

În anul 2013, OSCE adoptă un set de măsuri pentru creșterea încrederii în securitatea cibernetică (CBMs), fapt care reprezintă un succes în contextul cooperării internaționale. OSCE, ca organizație supranațională, devenită pionier în domeniu este și prima organizație regională care adoptă un set de astfel de măsuri. Aici se face referire la importanța respectării și aplicării dreptului european și internațional, dar şi la responsabilizarea statutului privind respectarea drepturilor omului şi a libertăţilor fundamentale în raport cu activitățile de promovare a securității cibernetice, atât în spațiul european, cât și în afara acestuia.

În anul 2014 se organizează primul hub pentru schimbul de informații din sectorul securității cibernetice, unde participă un număr de 57 de state din trei continente - America de Nord, Europa și Asia. Multe dintre aceste state investesc în capabilitățile ofensive și defensive din sectorul cibernetic, fapt care expune o dimensiune complexă a relațiilor interstatale, evidențiindu-se astfel trăsături specifice conceptului realismului. Dar odată cu utilizarea capacităților prin OSCE în operațiuni de recunoaștere și de informare, întreruperea rețelelor și serviciilor critice sau a capacităților de comandă și control, se dovedește încă o dată că tendința acestora este de a lua parte la construcția unui concept de colaborare supranațional.

Drept urmare, statele participante la OSCE lucrează la actualizarea și implementarea de măsuri de consolidare a încrederii, cu scopul de a reduce riscul de conflict - chiar și deschis, care decurge din utilizarea resurselor și a instrumentarului din arealul cibernetic. Măsurile sunt concepute pentru a face domeniul cibernetic mai transparent și cuantificabil, dar și din punct de vedere diplomatic prin adoptarea instrumentarului și mecanismelor potrivite cu scopul de evita orice formă a conflictului.

Este pus un accent deosebit pe evidențierea și promovarea nevoii de a oferi răspunsuri adecvate și la timp din partea autorităților naționale cu privire la amenințările cibernetice și cu privire la evoluția

acestora. Amenințările cibernetice pot veni din multe surse, iar pentru a limita și a dejuca succesul unor infracțiuni sau atacuri în acest mediu, se încearcă obținerea unui cadru unic și legitim de utilizare a resurselor în sectorul cibernetic.

Ocupând pentru perioada 2014 - 2019 funcția de șef de dosar UE în domeniul cibernetic, România a elaborat poziția UE în sectorul securității cibernetice, reprezentând Uniunea Europeană în negocierile din acest sector.

Totodată, în perioada 2015 - 2016, România a preluat Președinția Comitetului de Securitate, tratând cu rigurozitate problematica combaterii terorismului, reforma sectorului de securitate, guvernanța securității cibernetice, combaterea fenomenului criminalității cibernetice şi implementarea unor măsuri de creștere a încrederii în domeniul securității cibernetice în baza CBMs, precum și accentuarea nevoii de cooperare între autoritățile de aplicare a legii a Statelor Participante.

În urmărirea obiectivului de a proteja statele partenere și nu numai împotriva atacurilor teroriste, România s-a remarcat ca fiind, în ultimii ani, în cadrul OSCE, un lider pro-activ. În continuare, România își păstrează calitatea de monitor al priorităților naționale privind poziția în UE prin acordarea unui interes necondiționat:

- importanței conformării, alinierii și respectării dreptului internațional şi a drepturilor omului în asigurarea securității cibernetice;
- asigurării unei comunicări și transparențe internaționale privind securitatea cibernetică pentru obținerea unor rezultate comune alături de organizațiile internaționale;
- creării unui front comun cu actorii de securitate privind o mai bună guvernanță a internetului;
- promovării libertății de exprimare;
- facilitării dialogului între state în contextul atacurilor cibernetice iminente care pot duce la conflicte de natură politico-militară;

- performării sub OSCE ca platformă pentru schimbul de informații în domeniul securității cibernetice.

Octombrie 2016 marchează adoptarea Deciziei nr. 5/16 *privind Eforturile OSCE privind reducerea riscurilor care decurg din conflictele dezvoltate din utilizarea tehnologiilor informației şi a comunicațiilor*[1], obținută în urma prezentării acesteia de către Președinția în Exercițiu a Germaniei, cu ocazia reuniunii Consiliului ministerial al OSCE, organizat la Hamburg, în perioada 8-9 decembrie 2016.

V.3. Modele internaționale și organisme europene cu atribuții în domeniul securității cibernetice

În ultimii ani, atât organismele și instituțiile supranaționale, cât și cele naționale, pentru asigurarea unui nivel optim de securitate națională și internațională, pun un accent tot mai mare pe utilizarea noilor tehnologii care își aduc aportul prin apariția de soluții și sisteme inteligente, ce au ca obiectiv modernizarea infrastructurilor și sistemelor de guvernare, precum modelul eGuvernare sau Gov2.0. În acest context, în 12 februarie 2019, Departamentul Apărării al SUA a publicat pentru prima dată, probabil că și primul rezumat al Strategiei de Inteligență Artificială[2]. Strategia are ca scop primar utilizarea dezvoltării tehnologice în domeniul AI pentru a progresa din punct de vedere al securității și prosperității și subliniază modul în care Departamentul Apărării va utiliza AI în viitor.

Principiile cheie ale strategiei sunt accelerarea mecanismelor de furnizare a soluțiilor bazate pe AI și integrarea de astfel de soluții la nivel instituțional. Pentru a împlini aceste obiective și pentru a

1. OSCE, „DECISION No. 5/16 OSCE efforts related to reducing the risks of conflict stemming from the use of information and communication technologies", https://www.osce.org/cio/288086?download=true, accesat astăzi 04.05.2019.
2. U.S. Department of Defense, nr. NR-026-19, „New Strategy Outlines Path Forward for Artificial Intelligence", 12.02.2019;

dezvolta acest sector, Departamentul Apărării cooperează prin parteneriate strategice cu entități din mediul industrial, mediul academic, aliați și parteneri - toate acestea pentru o cultivare a unei forțe operaționale bazate pe soluții AI și pentru o aplicabilitate a acestor soluții, respectând codurile de etică și siguranță în sectorul militar. În aceeași măsură, cercetarea pentru obținerea de rezultate în domeniul roboticii, medicina aplicată, securitatea și siguranța națională sunt absolut relevante și necesare. Așadar, sunt utilizate sisteme AI pentru a oferi soluții, explicații raționale, dar și pentru a crea și inova în domenii cu problematici profunde sau abstracte, precum sunt muzica, arta vizuală, arta plastică. Pentru obținerea de rezultate cu un alt nivel de eficiență - raportat la rațiunea, simțirea și inteligența umană - se utilizează diverse metode de AI, cum ar fi căutarea spațiului de stat, rețelele neuronale, algoritmi genetici, rețele semantice și raționare prin analogie.[1] Această abordare este utilizată și în observarea, cercetarea, analizarea și investigarea spațiului cibernetic în ansamblul său.

Abordarea strategică a Departamentului Apărării pentru AI pune accentul pe livrarea și implementarea rapidă, iterativă și responsabilă a soluțiilor.

Așa cum revoluția industrială a schimbat modul de abordare la orice nivel în societate, tot așa inteligența artificială, fără dubii, va influența atât progresul și prosperitatea societății ce stă să răsară, cât și viitoarele strategii și manevre din teatrele de operațiuni militare ori conflictele militare. Această strategie a Statelor Unite ale Americii are ca scop realist asigurarea securității federațiilor constituite ori parteneriatelor în curs de derulare alături de aliații acesteia, unde este nevoită să adopte o poziția pro-activă și strategică pentru a prevala în ceea ce privește viitoarele câmpuri de luptă fizice ori virtuale.

AI a început deja să își facă simțită prezența la nivel societal și efectele AI nu își fac lipsită prezența nici în sectorul guvernamental, în

1. Mariusz Flasiński, *Introduction to Artificial Intelligence*, Edit. Springer, Elveția, 2016, pp.233-234.

tot ceea ce înseamnă operațiuni, pregătire, suport, recrutare, asistență medicală și multe altele. În acest context al utilizării tehnologiilor avansate de AI, trebuie luată în considerare nevoia de a evalua și de a testa capacitatea de a verifica deciziile unui astfel de sistem. Motivația principală este de a încuraja dezvoltarea acestor sisteme și de a construi încredere în raportul om / sistem informatic. Sistemele de monitorizare și control ale sistemelor de AI sunt esențiale mai ales în cazul în care acestea sunt utilizate cu un rol de susținere și validare (*diagnosticul medical, analiză de risc, testare de securitate*) și în situațiile în care acestea sunt operaționale și dețin calitatea de sistem autonom, în care pot lua decizii (*conducere autonomă, GIS*). În primul caz, raportul sau informațiile furnizate pot oferi un suport pentru luarea deciziei și chiar pentru a schimba traiectoria propusă de beneficiar, pe când în cel de-al doilea caz, este absolut necesar ca acest sistem cu capacitate decizională să poată furniza explicații foarte detaliate, granulare și structurate pentru a putea fi monitorizat și controlat de beneficiarul serviciilor sistemelor de AI.[1]

În cazul SUA, această Strategie a Departamentului de Apărare pentru Inteligență Artificială susține îndeaproape Strategia Națională de Apărare și face parte din eforturile globale ale acestui departament de a aduce la standarde cât mai înalte, prin modernizare, dezvoltare, cercetare și inovare, elementele componente din sectorul tehnologiei informației și a comunicațiilor. Motivația primordială a acesteia este apărarea valorilor, resurselor și integrității departamentului și a statului împotriva atacurilor cibernetice și a tehnologiilor în curs de dezvoltare.

Inteligența artificială reprezintă o arie de cercetare cu rezonanță în ceea ce privește asigurarea securității naționale în anii ce vor veni. În cazul României, în perioada 2015-2019,am identificat o singură

1. Wojciech Samek, Klaus-Robert Műller, „Towards Explainable Artificial Intelligence”, în *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, Edit. Springer, 2019, pp.8-9.

măsură luată de către instituțiile abilitate și direct interesate pentru a concepe strategii sau planuri naționale în acest domeniu, anume lansarea primei platforme de Inteligență Artificială la nivel european, în coordonarea Thales.

Unul dintre proiectele Comisiei Europene, intitulat AI4EU, lansat cu scopul construirii și dezvoltării platformei pilot a UE de Inteligență Artificială, are și un obiectiv strategic de mobilizare a întregii comunități europene de resort AI. Bugetul alocat este unul generos, de 20 mil. euro, drept urmare și așteptările sunt pe măsura investiției, iar Thales este nominalizat lider de proiect, coordonând astfel lansarea platformei. Odată cu câștigarea acestui proiect, Thales are și rolul de a promova colaborarea celor 79 organizații din cele 21 țări membre ale UE cu ceilalți parteneri strategici și operaționali, iar pe viitor de redimensionare activă a rețelei de parteneri în zona europeană.

Proiectul UE AI4EU a fost lansat în 01.01.2019. Cu această ocazie, CE are oportunitatea de a-și atinge obiectivele în materie de cercetare, inovare și dezvoltare cu ajutorul inteligenței artificiale și a sistemelor în care aceasta este utilizată. Un alt obiectiv este cel de operaționalizare și reconceptualizare a sectorului de dezvoltare tehnologică și industrială a UE pentru mobilizarea întregului ecosistem european, format din cei 79 parteneri din 21 țări, sub aceeași platformă cibernetică europeană, cu rolul de a oferi acces la resursele AI în UE pentru toți utilizatorii. Este adoptată metoda pașilor mărunți în această direcție, fiind un domeniu în explorare, dar care își poate aduce aportul la accelerarea competitivității industriale și identificarea pragmatică a adoptării AI în celelalte sectoare ale economiei. România a semnat aderarea, alături de celelalte state membre, la acest proiect mamut pe 10 aprilie 2018, cu ocazia evenimentului *„Digital Day”*, care a avut loc în Brussels, Olanda. Rolul acestei platforme este cel de a consolida poziția Europei în calitate de putere supranațională elitistă la nivel global în domeniul utilizării tehnologiei AI. Odată cu depășirea

acestei granițe tehnologice, au apărut noi provocări de ordin etic, deontologic și chiar moral.

Un proiect ca cel coordonat de organizația Thales, cu sediul în Franța, are un buget estimat la aproximativ 20 mil. euro pentru următorii trei ani, de unde reiese și importanța acordată de UE sectorului AI și a oportunităților din mediul cibernetic. Proiectul este unul pilot, care promite multe, printre care și crearea unui sistem de monitorizare a problemelor de ordin etic și care să emită rezultate și ipoteze ca fond de cercetare pentru a demistifica și expune problematica rolului cetățenilor țărilor membre UE într-o societate modernă, competitivă, avansată și bazată pe tehnologii și sisteme automate de inteligență artificială. În altă ordine de idei, se dorește și crearea unei culturi de îmbrățișare a AI într-un mod aplicabil și controlat[1].

Oportunitatea acordată de CE Grupului Thales de a coordona proiectul-vine și cu o asumare a CE și a tuturor partenerilor implicați de a popula această platformă de IE cu instrumentarul necesar, componentele tehnologice și de comunicații, module informaționale, date, informații și baze de date cu cunoștințele necesare în vederea operaționalizării, algoritmi de procesare și alte elemente ce pot duce la perfecționarea sistemului de IA. Avantajul dezvoltării unui asemenea sistem de AI este că partenerii implicați din cadrul comunității europene a TIC vor avea posibilitatea finalmente de a utiliza sistemul pentru generarea de resurse în mod direct. Un alt beneficiu pentru întreaga comunitate îl aduce comunitatea științifică edificată în cadrul proiectului, care va disemina conform nevoilor și posibilităților o asistență practică sectorului antreprenorial, de afaceri, de cercetare științifică și academică, sectorului industrial, sectorului militar, sectorului tehnologiei informațiilor și a comunicațiilor, sectorului

1. European Commission, Digital Single Market, „Artificial Intelligence: The AI4EU project launches on 1 January 2019"-12.12.2018, https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-ai4eu-project-launches-1-january-2019, accesat în data de 22.02.2019.

securității și multor altor sectoare și domenii cu un real și direct interes în inovare, dezvoltare și progres.

„Obiectivul acestui proiect de trei ani este de a promova colaborarea în cadrul ecosistemului AI din Europa, astfel încât părțile interesate să împărtășească, să utilizeze și să creeze valoare adăugată, prin promovarea unor noi abordări în sectoare strategice ale economiei europene, inclusiv robotică, sănătate, mass-media, agricultură și securitate cibernetică. Acest proiect va oferi, de asemenea, elemente esențiale pentru a ajuta la stabilirea unei agende strategice, puternice și cuprinzătoare în domeniul Inteligenței Artificiale, la nivel european."[1]

În acest context, coordonatorul departamentului de tehnologie al Grupului Thales, Marko Erman afirmă "*Suntem foarte mândri de încrederea acordată de Comisia Europeană companiei Thales pentru coordonarea proiectului AI4EU, proiect care va ajuta Europa să-și consolideze poziția de actor global în cursa pentru dezvoltarea celor mai bune tehnologii digitale și AI, în serviciul societății*[2]".

În ceea ce privește Direcțiile de Acțiune și Principalele Modalități pentru Asigurarea Securității Naționale a României, primele două premise vizează Consolidarea credibilității strategice și Asigurarea unui cadru legal adaptat. Așadar, analizând mediul global și național de securitate, este insuficientă recunoașterea amenințărilor cibernetice la modul general și punctarea acestor atacuri ca dimensiuni de interes pentru sectorul de informații, contrainformații şi de securitate.

Guvernul României, prin Hotărârea CSAT nr. 16/2013 și Hotărârea nr. 271/2013, a aprobat Strategia de securitate cibernetică a României şi Planul de acțiune la nivel național privind implementarea

1. George GMT, *„Lansarea primei platforme de Inteligenţă Artificială la nivel european, în coordonarea Thales"*, 20.02.2019, https://www.rumaniamilitary.ro/lansarea-primei-platforme-de-inteligenta-artificiala-la-nivel-european-in-coordonarea-thales, accesat astăzi 22.02.2019;
2. Marko Erman, THALES, *„Launch f First European Artificial Intelligence Platform Coordinated By Thales"*, 01.10.2019, https://www.thalesgroup.com/en/group/journalist/press-release/launch-first-european-artificial-intelligence-platform-coordinated, accesat astăzi 22.02.2019;

Sistemului național de securitate cibernetică, a luat măsuri incipiente de combatere sau de prevenire a unor situații care ar putea afecta securitatea națională. Totuși, abordarea acestei Strategii[1] nu este suficient de granulară și nu cuprinde arii de interes precum reziliența cibernetică sau dezvoltarea și inovarea tehnologiilor bazate pe inteligență artificială. Drept urmare, una dintre acțiunile UE care a venit în ajutorul statului român pe considerentul apărării cibernetice este *„Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat”*[2] care, în baza priorităților, acțiunilor strategice și a viziunii comune a UE, articulează cinci direcții strategice în vederea asumării provocărilor mai sus menționate:

- Reconceptualizarea rezilienței cibernetice;
- Aplanarea și combaterea fenomenului criminalității cibernetice;
- Revizuirea politicilor de securitate și apărare cibernetică precum și a capacităților de apărare corelate cu politica UE de securitate și apărare comună (PSAC);
- Revitalizarea sectorului industrial și tehnologic prin cercetare, inovare și dezvoltare în materie de securitate cibernetică;
- Emiterea de politici internaționale congruente a Uniunii Europene privind guvernanța și managementul spațiul cibernetic precum și promovarea valorilor fundamentale ale UE în acest areal.

Această strategie are ca obiectiv principal dezvoltarea infrastructurilor cibernetice în conformitate cu perspectiva UE și raportată la

1. Guvernul României, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013, *„Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică”*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesată în data de 21.02.2019.
2. Comisia Europeană, Bruxelles, 7.2.2013 JOIN(2013) 1 final, Comunicare Comună către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor – „Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat”, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52013JC0001&from=ro, accesată în data de 21.02.2019.

viziunea, conceptele şi politicile existente în sectorul apărării cibernetice emise şi aplicate la nivelul NATO şi UE. Așadar, este identificată o reală nevoie de colaborare din punct de vedere procedural cu state care dețin cunoștințe bazate pe experiențe mult mai ample decât ale României.

Urmare a punerii în aplicare a Strategiei, apare sistemul național integrat - Sistemul Naţional de Securitate Cibernetică (S.N.S.C.) în calitate de organism cu rol supervizor în ceea ce privește implementarea coerentă a tuturor măsurilor de prevenire şi reacție la atacurile cibernetice împotriva instituțiilor publice sau a entităților din sectorul privat. Acest sistem reunește sub aceeași viziune autoritățile şi instituțiile publice cu responsabilități şi capabilități concentrate în domeniul securității cibernetice.

Elementele de interes direct ale S.N.S.C. stau în asigurarea unei reacții reale la pericolele - *vulnerabilități, riscuri, amenințări, atacuri* - specifice din arealul cibernetic, care pot aduce atingere, uneori chiar gravă, securității infrastructurilor critice, securității infrastructurilor cibernetice naționale, inclusiv managementului consecințelor. Cele trei scopuri primare sunt *cunoașterea, prevenirea și contracararea*. Consider că lipsesc din această ecuație cel puțin două obiective esențiale asigurării unui nivel de securitate optim: conștientizarea și recuperarea.

Obiectivele din sarcina S.N.S.C. sunt regăsite în *„Planul de acțiune la nivel național privind implementarea S.N.S.C."*, document aprobat prin Hotărârea de Guvern nr. 271 din 15.05.2013, care conține planul de măsuri necesar a fi aplicat de entitățile de specialitate.

Strategia vine în ajutorul structurării obiectivelor congruente principiilor şi direcțiilor de acțiune într-un sens unitar pentru asumarea cunoașterii, identificarea mijloacelor de prevenire şi înlăturare sau diminuare a riscurilor şi amenințărilor adresate securității cibernetice în România.

Având ca obiectiv principal protecţia infrastructurilor IT&C din sectorul guvernamental, administrativ, public şi privat, *„Strategia de Securitate Cibernetică a României"* urmărește următoarele obiective:

- emiterea, actualizarea și republicarea cadrului normativ şi legislativ la dinamica provocărilor specifice în arealul cibernetic;
- stabilirea unui cadru național pentru creșterea securității infrastructurile cibernetice, cu o deosebită aplicabilitate în funcționarea infrastructurilor critice;
- creșterea nivelului de reziliență a sistemelor și infrastructurilor operaționale în spațiul cibernetic;
- dezvoltarea planului de cooperare a României în plan național, european şi global;
- dezvoltarea unei culturi de securitate cibernetică în rândul cetățenilor ce utilizează instrumentarul digital în raport cu domeniul cibernetic și conștientizarea acestora în raport cu posibilele vulnerabilități, riscuri, amenințări și atacuri existente în acest areal, precum și în vederea dobândirii de calități necesare securizării echipamentelor moderne de comunicații și tehnologia informației.

Cele cinci principii care stau la baza realizării securității cibernetice sunt:

- *„Coordonarea - activitățile se realizează într-o concepție unitară, pe baza unor planuri de acțiune convergente destinate asigurării securității cibernetice, în conformitate cu atribuțiile şi responsabilitățile fiecărei entități;*
- *Cooperarea - toate entitățile implicate (din mediul public sau privat) colaborează, la nivel național şi internațional, pentru asigurarea unui răspuns adecvat la amenințările din spațiul cibernetic;*
- *Eficiența - demersurile întreprinse vizează managementul optim al resurselor disponibile;*

- *Prioritizarea - eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susțin infrastructurile critice naționale şi europene;*
- *Diseminarea - asigurarea transferului de informații, expertiză şi bune practici în scopul protejării infrastructurilor cibernetice;*
- *Protejarea valorilor - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creștere a securității în spațiul cibernetic şi prezervarea dreptului la intimitate şi alte valori şi libertăți fundamentale ale cetățeanului;*
- *Asumarea responsabilității - toți deținătorii şi utilizatorii de infrastructuri cibernetice trebuie să întreprindă măsurile necesare pentru securizarea infrastructurilor proprii şi să nu afecteze securitatea infrastructurilor celorlalți deținători sau utilizatori;*
- *Separarea rețelelor - reducerea probabilității de manifestare a atacurilor cibernetice, specifice rețelei internet, asupra infrastructurilor cibernetice care asigură funcțiile vitale ale statului, prin utilizarea unor rețele dedicate, separate de internet"*[1].

Odată ce a fost identificată viziunea comună, principiile și obiectivele, se consolidează poziția *ENISA* și în ceea ce privește capacitățile naționale de realizare a rezilienței cibernetice. UE, în calitate de generator de securitate supranațional, va coordona în continuare alertele, evenimentele, incidente și atacurile cibernetice transfrontaliere cu un anumit grad de risc și o certă amploare, precum și identificarea mijloacelor optime de coeziune cu sectorul privat în acest domeniu de expertiză. Strategia UE este în mod natural însoțită de o propunere a unui pachet legislativ, care vizează în mod special stabilirea cerințelor minime comune în materie de Securitate a Rețelelor și Informației

1. Guvernul României, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013, *„Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică"*, pp.8-9, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesată în data de 21.02.2019.

(*NIS*) la nivel național, care aduce pe lângă nevoia de ratificare, un set de obligații adresate instituțiilor de resort din statele membre UE. În egală măsură este impusă înființarea unor mecanisme centrale de conștientizare, prevenire, monitorizare rezilientă și de răspuns cu capacitatea activă de schimb de informații și colaborare în rețeaua autorităților naționale de specialitate în domeniul securității rețelelor și informației în format digital. Interesul Comisiei a căzut asupra nevoii de îmbunătățire a pregătirii și a implicării sectorului privat, deoarece rețelele sunt într-o mare măsură aparținătoare sectorului privat, iar această colaborare este esențială pentru promovarea securității cibernetice și creșterea culturii de securitate cibernetică a populației.

În ceea ce privește abordarea strategiei de către statele membre și reconsiderând la nivel național complexitatea problematicii, precum și implicarea directă sau indirectă a actorilor statali și non-statali, supravegherea centralizată printr-un organism unic sau printr-un sistem coordonat la nivel european nu pare a fi soluția potrivită. Cu sprijinul entităților europene, atât guvernele cât și administrațiile naționale sunt capabile și provocate să organizeze activități de conștientizare, prevenție și reacție în cazul unor evenimente sau atacuri în mediul cibernetic la nivelul circumscripției fiecărui stat. Instituțiile specializate ale statelor membre UE cunosc contextul de securitate național și capacitatea, respectiv nevoile naționale de securitate și sunt cele îndreptățite să-și lărgească rețeaua de parteneri cu organizații din sectorul privat, dar și cu organizații profesionale / asociații de profil. Acest lucru poate fi realizat și grație canalelor de comunicare sau colaborării administrative și publice. Datorită caracterului transfrontalier al infracțiunilor și al riscurilor generate în mediile virtuale, validarea unei acțiuni eficiente și redundante la nivel național este bazată pe o strânsă colaborare a acestor state cu instituțiile UE de profil, iar în unele cazuri se impune o acțiune mai amplă, în care UE, în calitate de putere supranațională, să strângă toate capacitățile și resursele puse la dispoziție de statele membre UE pentru a crea un

front comun de răspuns - acțiune scalabilă în funcție de anamneza de securitate a fiecărui eveniment în parte.

Securitatea cibernetică poate fi abordată prin tratarea într-un mod exhaustiv a celor trei piloni principali - *NIS* , *Aplicarea legii*, *Apărare cibernetică*- reglementați prin cadre juridice diferite, explicate succint și schematic în Figura nr.21. *Diagrama sistemului de securitate cibernetică al UE.*

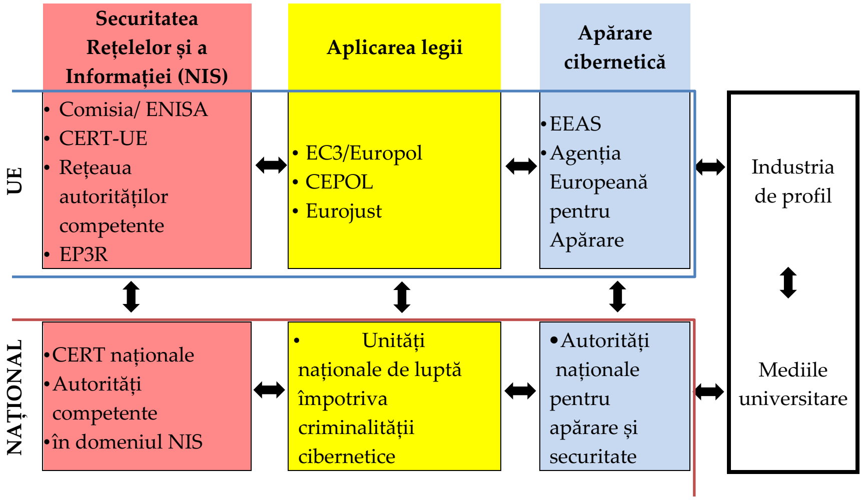


Figura nr.21. Diagrama sistemului de securitate cibernetică al UE

V.4. Modele și organisme naționale cu atribuții în domeniul securității cibernetice

În România, activitatea Sistemului Naţional de Securitate Cibernetică este coordonată la nivel strategic de CSAT[1]. Guvernul României, prin Ministerul pentru Societatea Informațională, asigură coordonarea

1. Legea de Organizare a Consiliului Suprem de Apărare a Ţării, Legea nr. 415 din 27 iunie 2002 *privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării*, http://csat.presidency.ro/, accesat în data de 14.03.2019.

celorlalte autorităţi publice în vederea realizării coerenței politicilor şi implementării strategiilor guvernamentale în domeniu.

Sistemul Naţional de Securitate Cibernetică are în componență, pe de-o parte, autoritățile publice cu competențe în sectorul securității cibernetice, instituții precum Secretarul Consiliului Suprem de Apărarea Ţării, Ministerul pentru Societatea Informațională, Ministerul Afacerilor Externe, Ministerul Afacerilor Interne, Ministerul Apărării Naționale, Serviciul de Informații Externe, Serviciul Român de Informații, Serviciul de Protecție şi Pază, Serviciul de Telecomunicații Speciale și Oficiul Registrului Național pentru Informații Secrete de Stat, iar pe de altă parte actori non statali din mediul asociativ non-guvernamental, profesional şi din mediul privat - de afaceri.

SNSC, prin mecanismul propriu de implementare, în plan pro-activ / reactiv, este asigurat prin funcționalitatea celor două organisme strategic-operative, respectiv prin Consiliul Operativ de Securitate Cibernetică (COSC) și Grupul de Suport Tehnic (GST).

Mecanismul de implementare a strategiei de securitate cibernetică la nivel național este asigurat prin:

- *„**Consiliul Operativ de Securitate Cibernetică (COSC)**, al cărui regulament de organizare şi funcționare a fost aprobat prin Hotărârea CSAT nr. 17/2013. Acesta este format din reprezentanți la nivel de secretar de stat din cadrul instituțiilor sistemului de securitate naţională, inclusiv ai MAE şi care se ocupă de coordonarea unitară a SNSC. Funcția de coordonator tehnic al COSC este asigurată de către Serviciul Român de Informații în calitate de autoritate naţională în domeniul securității cibernetice prin intermediul Centrului Național Cyberint (CNC), care informează operativ COSC cu privire la apariția incidentelor de tip cibernetic care pot aduce atingere securității naționale. Consiliul raportează către CSAT, anual sau ori de câte ori situația o impune, cu privire la acțiunile întreprinse, precum şi la evoluțiile înregistrate în spațiul cibernetic, în special cu referire la incidente sau atacuri cibernetice*

- ***Grupul de Suport Tehnic (GST)****, are în alcătuirea sa reprezentanți la nivel de expert din cadrul instituțiilor sistemului de securitate națională reprezentate în cadrul COSC"*[1].

Cu toate că prin acțiunea sa, Curtea Constituțională a României (CCR) din 27 ianuarie 2015 critică Legea privind securitatea cibernetică, care aparent contravine prevederilor Constituției privind noțiunea statului de drept, principiului legalității, dreptului la viața intimă, familială şi privată și în aceeași măsură contravine principiului secretului corespondenței, totuși aceasta recunoaște funcționalitatea și utilitatea autorității naționale în domeniul securității cibernetice. De menționat în acest context este că pentru a garanta aceste drepturi ar trebui să fie înființată o entitate în parteneriat colaborativ civil şi în paralel cu *Centrul Naţional de Securitate Cibernetică* (CNSC), care este operațional deja în cadrul Serviciului Român de Informații, având în subordine personal militar. Acest organism de răspuns la atacuri cibernetice reprezintă punctul de contact și susținătorul cadrului de cooperare și relaționarea cu organismele de profil similare în UE și extenso.

„Un alt suport în domeniul securității cibernetice este reprezentat de ***Sistemul Naţional de Alertă Cibernetică (SNAC)*** aceasta reprezintă principalul mijloc al SNSC destinat prevenirii şi contracarării activităților de natură să afecteze securitatea cibernetică, *care instituie nivelurile de alertă cibernetică (NAC), pe baza evaluării procesului de management al riscurilor la adresa securității cibernetice a României. Coordonarea tehnică a activității SNAC şi controlul măsurilor specifice fiecărui nivel de alertă, propuse în cadrul COSC şi aprobate de CSAT, se realizează de către Centrul Național Cyberint (CNC)"*[2]. Din punct de vedere tehnic, activitatea SNAC, precum şi monitorizarea măsurilor propuse

1. Ministerul Afacerilor Externe, Securitate Cibernetică, „Strategia de securitate cibernetică a României", https://www.mae.ro/node/28367, accesat în data de 14.03.2019.
2. Andreea-Maria Tirziu, „Protection and security of information at the level of national public authorities from Romania", în *MPRA Munich Personal RePEc Archive*, Munchen, 2015, p.127, https://mpra.ub.uni-muenchen.de/77711/1/MPRA_paper_77711.pdf, accesat astăzi 14.03.2019;

pentru fiecare nivel de alertă, examinate în cadrul COSC şi aprobate de CSAT, se realizează de către CNC.

În România, în temeiul art. 108 din Constituția României, republicată, și al art. 11 alin. (1) și (2) din Ordonanța Guvernului nr. 57/2002 privind cercetarea științifică și dezvoltarea tehnologică, aprobată cu modificări și completări prin Legea nr. 324/2003, cu modificările și completările ulterioare, prin Hotărârea de Guvern nr.494 din 02 iunie 2011 *privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO*, apare conform art.1 *„structura independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice"*[1]. Două dintre cele mai importante atribute CNC sunt capacitatea de a emite alerte și posibilitatea de a emite atenționări privitoare la acțiunile premergătoare atacurilor cibernetice. CNC i s-au oferit posibilitatea și resursele necesare în ceea ce privește conștientizarea, măsurile de prevenție, capacitățile de analiză, posibilitățiі de detecție şi reacție la evenimente, incidentele și atacurile în spectrul de securitate cibernetică - măsuri raportate în mod direct sistemelor informatice care reprezintă o nevoie funcțională și operațională de utilitate publică ori raportate la diversele servicii prezente în societatea informațională contemporană. CERT-RO este coordonat de Guvernul României prin intermediul Ministerul Comunicațiilor și Societății Informaționale (MCSI)[2] și este finanțat integral de la bugetul de stat[3].

COSC raportează eșalonului superior CSAT, de fiecare dată când situația o impune și regulat o dată pe an, cu privire la activitatea COSC, precum şi la progresul și atingerea obiectivelor propuse în

1. CERT-RO, Hotărâre CSAT, Art.1, *„Regulament privind organizarea și funcționarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO"*, p.3, https://cert.ro/uploads/rof.pdf, accesat în data de 14.03.2019.
2. CERT-RO, „RFC 2350 description for CERT-RO", p.3, https://cert.ro/vezi/document/RFC2350-CERT-RO, accesat în data de 14.03.2019.
3. CERT-RO, Buget, https://www.cert.ro/doc/buget, accesat în data de 14.03.2019.

arealul cibernetic, cu acordarea unei atenții deosebite evenimentelor, incidentelor și atacurilor cibernetice la nivel național.

V.5. Strategii de securitate cibernetică în zona UE în raport cu restul lumii

„Strategia Globală a UE pentru Politică Externă și de Securitate din 2016”[1] include domeniul *“cyber”* printre prioritățile centrale. Uniunea Europeană își concentrează tot mai mult atenția asupra domeniului securității cibernetice, asupra capacitării și sprijinirii Statelor Membre ale UE/SME pentru crea un scut protector împotriva amenințărilor cibernetice, păstrând în același timp o transparență a comunicațiilor și un spațiu cibernetic deschis, liber și sigur. Problematica ”cyber” este regăsită în toate domeniile politice, având ca scop consolidarea resurselor și capacităților cibernetice în operațiunile și misiunile PSAC.

Cadrul politic de la nivel Uniunii Europene în domeniul securității cibernetice are în atenție implementarea și monitorizarea Strategiei UE pentru Securitate Cibernetică, strategie care a fost evidențiată în 2017 împreună cu poziția Comisiei privind o abordare coordonată a incidentelor cibernetice transfrontaliere la scală largă. Strategia UE pentru securitate cibernetică reprezintă viziunea globală a UE cu privire la cele mai pertinente mijloace de prevenire şi guvernare a disensiunilor apărute în arealul cibernetic.

„Strategia definește viziunea UE în materie de securitate cibernetică prin intermediul a cinci priorități:

- *Obținerea unei reziliențe a infrastructurilor cibernetice*
- *Reducerea drastică a criminalității informatice*

1. EUEA, EU Global Strategy, „O strategie globală pentru politica externă și de securitate a Uniunii Europene”, http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf, accesat în data de 04.07.2018.

- *Dezvoltarea unei politici de apărare împotriva atacurilor cibernetice și a capacităților necesare în contextul politicii de securitate şi apărare comună (PSAC)*
- *Dezvoltarea resurselor industriale și tehnologice necesare pentru securitatea cibernetică*
- *Stabilirea unei politici internaționale coerente a Uniunii Europene privind spațiul cibernetic și promovarea valorilor fundamentale ale UE*"[1].

V.5.1. Cooperarea comunitară și internațională.

În vederea abordării și adoptării „*Strategiei de Securitate Cibernetică a UE*", s-a emis la Bruxelles, în 11.05.2017, de către Consiliul UE, Foaia de parcurs ca plan de măsuri structurat cu obiectivul de a promova inițiativa în vederea urgentării acțiunilor cibernetice desfășurate de către Președinția UE. Acest „Road Map" este structurat în șase secțiuni, fiecare secțiune având un plan de măsuri bine structurat privind următoarele aspecte:

A. Valori şi prosperitate (tradus. EN, *Values and Prosperity*);
B. Obținerea rezilienței cibernetice (tradus. EN, *Achieving Cyber Resilience*);
C. Criminalitatea cibernetică (tradus. EN, *Cybercrime*);
D. Politica de Securitate şi Apărare Comună / PSAC (tradus. EN, *Common Security and Defence Policy /CDSP*)
E. Industrie şi tehnologie (tradus. EN, *Industry and Tehnology*);

Pe 6 noiembrie 2018, în urma unei reuniuni sub forma unei întâlniri de lucru, MoU, ENISA, EDA, Europol, Serviciul de urgență în domeniul calculatoarelor, Echipa de răspuns la incidente cibernetice, agențiile și organismele UE (CERT-UE) s-au reunit la sediul CERT-UE.

1. Comisia Europeană, European Union External Action, „Planul UE în domeniul securității cibernetice pentru protejarea internetului deschis, a libertății online și a oportunităților generate de internet", http://europa.eu/rapid/press-release_IP-13-94_ro.htm, accesat în data de 26.04.2019.

Întâlnirea a avu ca scop comun, actualizarea și schimbul de informații reciproc asupra evoluțiilor din sectorul securității cibernetice relevante și evaluarea progreselor înregistrate în cadrul MoU, care reprezintă un cadru de cooperare care vizează mobilizarea sinergiilor dintre cele patru organizații pentru a realiza un spațiu cibernetic sigur.

Aceștia au convenit asupra unei foi de parcurs elaborate de grupul de lucru al MoU cu activități și rezultate concrete în cursul anului 2019. Directorul executiv al ENISA, Udo Helmbrecht, a declarat: *„Salut deciziile luate astăzi. Cu toții am căzut de acord asupra unei foi de parcurs concrete pentru lunile următoare, care se axează pe activități comune. exercițiul Cyber Europa 2020, precum și alte exerciții tehnice conexe pe care ENISA le va organiza. Suntem hotărâți să ducem această cooperare la nivelul următor"*.

Se va pune accentul în primul rând pe o apropiere mai strânsă în domeniul formării și exercițiilor cibernetice, pe consolidarea capacității de cooperare și îmbunătățirea schimbului de informații privind proiectele și evenimentele respective, în vederea completării activității celor patru parteneri și evitarea dublelor eforturi.

În urma acestei întâlniri, s-a stabilit un acord asupra faptului că aceasta a reprezentat o etapă importantă pentru intrarea într-o nouă eră a colaborării și un prim pas important în punerea în practică a cadrului de cooperare[1].

Acest tip de activitate este unul orientat nu doar spre o colaborare eficientă, ci și spre o unificare a forțelor cu un scop și o viziune comună.

Componenta principală a strategiei globale de securitate cibernetică a Uniunii Europene este reprezentată de Directiva NIS[2]. Aceasta

1. ENISA, „EU cybersecurity organisations agree on 2019 roadmap", 2018, https://www.enisa.europa.eu/news/enisa-news/eu-cybersecurity-organisations-agree-on-2019-roadmap, accesat în data de 26.04.2019.
2. *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.*

a fost emisă în scopul asigurării unui nivel de securitate a rețelelor şi a informației în EU la valori pertinente dacă nu chiar ridicate, de unde apare și perspectiva de dezvoltare a securității mediilor virtuale şi a rețelelor private, dar şi a echipamentelor de comunicații și tehnologia informației pe care societatea contemporană și economia europeană se bazează. Documentul legislativ a fost aprobat formal de către Consiliu și Parlamentul European/PE și a fost publicat în Jurnalul Oficial al UE la 19 iulie 2016.

Statele membre au avut la dispoziție 21 de luni de la data intrării în vigoare pentru a implementa directiva și încă șase luni pentru a identifica operatorii de servicii esențiale. În România acest lucru a avut loc pe 16 mai 2018, *„Plenul Camerei Deputaților, ca for decizional, a aprobat proiectul de lege inițiat de Ministerul Comunicațiilor și Societății Informaționale, ce vizează transpunerea la nivel național a Directivei NIS a Uniunii Europene (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune* - *directiva NIS.*[1]” Proiectul de lege a fost transmis spre promulgare Președintelui României. Actualmente, ca urmare a alinierii României la legislația internațională pe această problematică, în baza Directive NIS - *este primul act emis de cvorumul legislativ al UE cu privire la securitatea cibernetică*- care stabilește o bază legală pentru crearea de condiții de concurență echitabile pentru securitatea cibernetică în statele membre. România are, începând cu 12 ianuarie 2019[2], legislație ratificată și conformă în acest domeniu[3]. Actul normativ are o importanță deosebită pentru România, deoarece transpune la nivel

1. Ministerul Comunicațiilor și Societății Informaționale, „Legea pentru transpunerea Directivei NIS a fost adoptată în Parlament”, https://www.comunicatii.gov.ro/legea-pentru-transpunerea-directivei-nis-a-fost-adoptata-in-parlament/, accesat în data de26.04.2019.
2. certSIGN, „Din această lună, România are o Lege pentru Securitatea Reţelelor şi Sistemelor Informatice”, https://www.certsign.ro/ro/din-aceasta-luna-romania-are-o-lege-pentru-securitatea-retelelor-si-sistemelor-informatice, accesat în data de 26.04.2019.
3. Legea nr. 362/2018 *privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.*

național Directiva NIS nr. 1148/2016 şi aliniază țara noastră la un cadru european comun de răspuns la incidente de securitate cibernetică. Aplicarea Directivei în strânsă cooperare între Comisia Europeană și statele membre face ca eforturile vizate să asigure dezvoltarea rețelei CSIRT. România, în calitatea sa de stat membru UE, a adoptat prin Parlamentul României și a desemnat autoritatea națională, Ministerul Comunicațiilor şi Societății Informaționale, denumit în continuare MCSI, la propunerea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică, care au stabilit o strategie de abordare a amenințărilor cibernetice.

Legea nr. 362/2018[1] consolidată la data de 01 februarie 2019, având la bază publicarea din Monitorul Oficial, Partea I nr. 21 din 09 ianuarie 2019 şi incluzând modificările aduse prin Ordonanța nr. 2 din 03 februarie 2019 și un ultimul amendament în 31 ianuarie 2019, clarifică sincopele de transpunere a Directivei în legislația națională.

Directiva NIS are ca obiectiv strategic creșterea cooperării între statele membre UE şi urmărește stabilirea și uniformizarea obligativităților de aliniere la standardele proprii (UE) de securitate atât pentru beneficiarii și furnizorii de servicii critice ori esențiale societății informaționale, cât şi pentru furnizorii de servicii din mediul cibernetic. Furnizorii de servicii esențiale sunt preponderent activi în sectoarele infrastructurilor critice, precum sectorul energetic, medical, financiar-bancar și cel al transporturilor.

Bazate pe gradul ridicat de risc pe care o aduce indisponibilitatea serviciilor sau perturbarea acestora în raport cu nevoile fundamentale ale societății și economiei contemporane, obligațiile Directivei sunt mai exigent concepute pentru operatorii de servicii esențiale decât pentru furnizorii de servicii digitale, cărora printr-o armonizare a

1. Camera Deputaților, PL-x nr. 280/2018, „Proiect de Lege privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice", http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?idp=17075, accesat în data de 04.07.2019.

cerințelor le sunt impuse reguli specifice, similare dacă nu chiar identice, oriunde ar opera în spațiul UE.[1]

Fac obiectul Directivei 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 *privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*, atât diseminarea, cât și schimbul de date și informații cu caracter special sau sensibil, precum sunt cele privind infracțiunile sau atacurile împotriva sistemelor informatice și de comunicații. „*Obiectivele acestei directive constau în armonizarea sistemelor de drept penal ale statelor membre în ceea ce privește atacurile împotriva sistemelor informatice, prin instituirea unor norme minime privind definirea infracțiunilor și a sancțiunilor relevante, precum şi de a îmbunătăți cooperarea dintre autoritățile competente, inclusiv poliția şi alte servicii specializate de aplicare a legii din statele membre, precum şi agențiile şi organismele specializate competente ale Uniunii, cum ar fi CERT EU - Centrul European de Răspuns la Incidente Cibernetice, Eurojust, Centrul pentru Combaterea Criminalității Informatice (EC3) al Europol respectiv Agenția Uniunii Europene pentru Securitatea Rețelelor şi a Informațiilor (ENISA) care are sediul central la Heraklion în Grecia*”[2], Forumul European pentru Statele Membre (EFMS).

Data de 4 septembrie 2015 a reprezentat termenul limită pentru transpunerea Directivei 2013/40/UE *privind atacurile împotriva sistemelor informatice* în legislația naţională a statelor membre UE. În acest context, pentru a facilita transpunerea Directivei în legislație națională, Comisia Europeană a desemnat și întrunit sub forma unei întâlniri de lucru un grup de specialiști, experți și practicieni din toate statele membre UE, care au avut exact acest rol, consultativ.

1. MAE, „Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora”, https://www.mae.ro/node/28369, accesat în data de 04.07.2018.
2. Jurnalul Oficial al Uniunii Europene, DIRECTIVA 2013/40/UE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, L 2018/8 RO, 14.08.2013, p.8.

„În CDPF actualizat au fost identificate șase domenii prioritare. Obiectivul primordial al acestui cadru de politici este dezvoltarea capabilităților de apărare cibernetică, precum și protejarea rețelelor de comunicații și informații din cadrul PSAC a UE. Printre celelalte domenii prioritare se numără: formarea și exercițiile, cercetarea și tehnologia, cooperarea civil-militară și cooperarea internațională. În domeniul formării, accentul se pune pe îmbunătățirea activităților de formare în domeniul apărării cibernetice desfășurate de statele membre, precum și a activităților de formare în vederea creșterii gradului de conștientizare cu privire la domeniul cibernetic la nivelul lanțului de comandă din cadrul PSAC. De asemenea, este important ca dimensiunea cibernetică să fie abordată în mod corespunzător în cadrul exercițiilor pentru a se îmbunătăți capacitatea UE de a reacționa la crizele cibernetice și hibride, prin îmbunătățirea procedurilor decizionale și a disponibilității informației. Spațiul cibernetic este un domeniu în rapidă evoluție, iar noile evoluții tehnologice trebuie să fie sprijinite, atât în domeniul civil, cât și în domeniul militar. Cooperarea civil-militară în domeniul cibernetic este esențială pentru a se asigura un răspuns coerent la amenințările cibernetice. Nu în ultimul rând, consolidarea cooperării cu partenerii internaționali ar putea contribui la consolidarea securității cibernetice atât în UE, cât și în afara acesteia, precum și la promovarea principiilor și valorilor UE."[1]

Primul exercițiu cibernetic pan-european, numit "*Cyber Europe Exercises*"[2], a fost desfășurat în 2010 sub monitorizarea ENISA. Au fost implicate aproximativ 600 de organisme europene din 29 de ţări membre ale UE şi EFTA. Cu această ocazie, s-a elaborat și lansat de către ENISA, *„Metodologia de identificare a ICIN-urilor"*. Exercițiul s-a desfășurat în 2010, 2012, 2014, 2016, 2018 și urmează să se desfășoare și în 2020. În perioada 06-07 iunie 2018, aproximativ 900 participanți

1. Secretariatul General al Consiliului Uniunii Europene, Bruxelles, „Cadrul de politici al UE pentru apărarea cibernetică (actualizare 2018)", 19.11.2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/ro/pdf, p.8, accesat în data de 27.04.2019.
2. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme, accesat în data de 22.07.2017.

din 28 de state membre UE și 2 state EFTA/AELS au participat la exercițiul ”Cyber Europe 2018”, organizat de ENISA[1]. CERT-RO a fost desemnat coordonatorul exercițiului „Cyber Europe 2018” în România, acesta deținând și calitatea de punct național de contact în domeniu.

Merită menționată inițiativa din 2 mai 2019 prin care CERT-RO a lansat un număr scurt unic „1911”, care poate fi apelat indiferent de rețea și prin intermediul căruia vor putea fi transmise informații și vor putea fi raportate evenimentele, incidentele și atacuri desfășurate în arealul cibernetic ori din rețelele publice/private. Nu există restricții privind persoana care apelează la acest număr, aceasta putând fi de la simplul utilizator de echipamente până la administratorul organizației din sectorul privat sau public. Acest număr scurt „1911” este interfața unui Call Center ce furnizează o asistență primară și consultanță în vederea identificării situației de fapt, diagnosticării și remedierii în măsura posibilităților tehnice. Este încurajată alertarea tuturor cazurilor ce implică (in)securitatea cibernetică din partea oricărui tip de organizație - publică/privată - și a cetățenilor sau a utilizatorilor. Un exemplu de atac la care se poate răspunde este tipul de campanie de colectare de date direcționată spre organizațiile din sectorul privat care gestionează date sensibile, date cu caracter personal sau chiar secret de stat și a căror accesare sau pierdere poate aduce pierderi considerabile persoanelor, partenerilor de afaceri, comunității economice sau statului. Aceștia se asigură că toate datele care vor fi extrase din aceste notificări vor sta la baza unor campanii de informare și alertare pentru alți posibili utilizatori vulnerabili, care pot deveni victime ale unor atacuri similare.

Exercițiul coordonat de ENISA a adus în prim plan concretizarea și funcționalitatea mecanismelor de cooperare naționale şi interna-

1. ENISA, „CYBER EUROPE 2018: AFTER ACTION REPORT - Findings from a cyber crisis exercise in Europe”, 2018, p.6, https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report/at_download/fullReport, accesat în data de 27.04.2019.

ționale prin aplicarea procedurilor operaționale adoptate în cazul alertei de securitate cibernetică, unde aproximativ 60% din totalul de 892 participanți au avut atribuții în domeniul securității cibernetice, au provenit din mediul privat și au răspuns alături de participanții din mediul guvernamental.

Contextul legislativ este extrem de important, motiv pentru care importanța aplicării dreptului internațional, a drepturilor și libertăților fundamentale ca bază pentru o securitate sporită în spațiul cibernetic, cooperarea statelor membre în atribuirea atacurilor cibernetice și în identificarea și urmărirea penală a autorilor sunt esențiale pentru a putea răspunde clar la provocarea reprezentată de criminalitatea cibernetică.

Eforturile vizează în mod special:

- asigurarea accesului rapid la dovezile electronice în investigațiile penale
- punerea în aplicare a măsurilor practice și legislative identificate pentru o mai bună cooperare între autoritățile guvernamentale și cu furnizorii de servicii.

UE a lansat Agenda Europeană pentru Securitate, iar Comisia Europeană în 2016 a comunicat[1] punerea în exercițiu a *„Agendei europene privind securitatea"* cu scopul principal de a combate actele de terorism cibernetic și de a promova formarea unui trunchi comun european pentru garantarea unui nivel de securitate efectivă și autentică, care include domeniul *„cyber"* printre prioritățile centrale, în principal în ceea ce privește combaterea criminalității cibernetice, pornografiei infantile on-line, consolidarea capabilităților de investigație în me-

1. Comisia Europeană, Bruxelles, 20.04.2016, COM(2016) 230 final, COMUNICAREA COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIUL EUROPEAN ȘI CONSILIU, *„Punerea în aplicare a Agendei europene privind securitatea pentru a combate* capacităților (CDP) și a *Planului de dezvoltare a capacităților civile (CCDP)*, statele membre *terorismul și a deschide calea către o uniune a securității efectivă și autentică"*, https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0021.02/DOC_1&format=PDF, accesat în data de 27.04.2019.

diul cibernetic. Totodată, Comisia Europeană, în 16 mai 2017, aduce în prim plan o nouă abordare privind interoperabilitatea sistemelor de informații prin prezentarea celui de-al șaptelea *„Raport privind progresele înregistrate către o uniune a securității efectivă și autentică”*[1]. În contextul Raportului, s-a analizat aplicabilitatea cadrului de politici de securitate cibernetică, luându-se în considerare și inițiativele UE în domeniul securității și apărării. Aici poate fi menționat *„procesul anual coordonat de revizuire privind apărarea (CARD), cooperarea structurată permanentă (PESCO), Fondul european de apărare (FEA) și pactul privind PSAC civilă, precum și revizuirea din 2018 a planului de dezvoltare a solicitat actualizarea cadrului de politici al UE pentru apărarea cibernetică. Consiliul Europei, a emis Cadrul de politici al UE pentru apărarea cibernetică (actualizare 2018), adoptat de Consiliu la cea de a 3652-a reuniune a sa, desfășurată la 19 noiembrie 2018”*[2].

Aspectele CSDP din Strategia de Securitate Cibernetică a UE și strategia de apărare cibernetică sunt tratate de Grupul Politico-Militar (PMG) şi Comitetul Politic şi de Securitate (PSC/COPS).

Problematica dezvoltării capabilităților de apărare cibernetică este tratată cu caracter neregulat și cu ocazia întrunirii Comitetului Militar al UE (EUMC) sau în cadrul întrunirilor organizate de Agenția Europeană de Apărare.

Strategia UE pentru securitate cibernetică revizuită este o nouă oportunitate pentru UE de a răspunde conform provocărilor contextual generate de riscurile de securitate cibernetice, de a consolida strategic dezvoltarea și creșterea încrederii în piața unică digitală (DSM), respectiv de a comunica la nivel internațional valorile fun-

1. Comisia Europeană, Comunicat de presă, „Agenda europeană privind securitatea: Comisia prezintă o nouă abordare privind interoperabilitatea sistemelor de informații”, http://europa.eu/rapid/press-release_IP-17-1303_ro.pdf, accesat în data de 27.04.2019.
2. Secretariatul General al Consiliului Uniunii Europene, Bruxelles, „Cadrul de politici al UE pentru apărarea cibernetică (actualizare 2018)”, 19.11.2018, p.3, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/ro/pdf, accesat în data de 27.04.2019.

damentale ce rezonează în contextul de securitate unde strategia își desfășoară interesul pentru spațiul cibernetic.

Rezultatele nu contenesc să apară, interesul acordat de sectorul guvernamental, privat și public-privat în consolidarea securității spațiului cibernetic în ultimii ani dezvoltă o reală creștere a încrederii în activitățile economice, financiare, de dezvoltare a serviciilor și fluxurilor informaționale în arealul cibernetic din circumscripția de securitate a UE.

Concluzii preliminare

Studierea implicațiilor aduse de diplomația digitală și diplomația cibernetică, în mod natural, ne duce la nevoia de aprofundare a influențelor politicii europene privind securitatea informației electronice în actuala stare geopolitică globală. Primul aspect care iese în evidență este aportul adus de președinția României și personalul guvernamental (MAI, MAE, MECT șamd.) în cadrul UE, dar și a statelor partenere cu care țara noastră colaborează.

Este imperios necesar să cunoaștem care este jurisdicția MAE în raport cu impactul diplomatic român în sectorul de securitate cibernetică. Pe de altă parte, în contextul României ca stat membru în Uniunea Europeană, trebuie învederată capacitatea de influențare din partea instituțiilor supranaționale europene în raport cu suveranitatea politică, economică și de securitate a statului.

Pentru a exprima cât mai coerent această relație și capacitatea de interdependență, este nevoie să observăm pe fiecare nivel al guvernanței spațiului cibernetic provocările, metodele și tipurile de controale conceptuale unice în raport cu reziliența cibernetică, înțelegând capacitatea de furnizare permanentă a rezultatului de securitate dorit, care se referă la o alianță, o națiune, o organizație sau chiar la un sistem informațional specific. După cum s-a constatat, pentru ca

reziliența cibernetică să fie eficientă, aceasta trebuie abordată în mod holistic pe toate nivelurile existente și în paralel.

Elementele de noutate sunt aduse de analiza problematicii securității cibernetice din perspectiva organismelor supranaționale prin entitățile internaționale de profil şi implicarea României în calitate de membru proactiv în domeniu, context în care am realizat un studiu comparativ a rezilienței cibernetice și a securității cibernetice pentru a înțelege poziția României în raport cu Uniunea Europeană - UE, Organizația Tratatului Atlanticului de Nord - NATO, CONSILIUL EUROPEI – CoE și Organizația pentru Securitate și Cooperare în Europa - OSCE.

Pentru a aduce clarificări, am considerat necesară abordarea și aprofundarea modelelor internaționale și a organismelor europene cu atribuții în domeniul securității cibernetice în contextul utilizării noilor tehnologii care își aduc aportul prin apariția de soluții și sisteme inteligente, care au ca obiectiv modernizarea infrastructurilor și sistemelor de guvernare, mai ales a organismelor supranaționale, precum modelul Statelor Unite ale Americii sau a Uniunii Europene. În aceeași ordine de idei, au fost expuse și modelul și organismele naționale din România cu atribuții în domeniul securității cibernetice, unde, cu toate că s-au identificat pași semnificativi în direcția construcției structurilor de profil de securitate cibernetică, s-a identificat o lipsă masivă de capital financiar și soluții de securitate și intelligence adoptate ori dezvoltate.

Cu toate că România s-a aliniat nu doar legislației internaționale, dar și normativelor europene, până în prezent, în comparație cu alte construcții supranaționale, implicarea strategică și operațională este dusă la nivel de existență, nu și de performanțe. Șansele de evoluție în această direcție atât pentru România cât și pentru întreaga UE sunt date și de cooperarea comunitară internațională.

Se identifică nevoia unei implicări pro-active, pe termen mediu și lung, din partea întregului front comun al UE. Planurile de măsuri

existente, emise de Consiliul UE, datorită progresului tehnologic în domeniul intelligence și al securității cibernetice, trebuie actualizate și completate.

Capitolul VI.
Studiu de caz – Cultura de securitate cibernetică în România

Într-o proporție covârșitoare, aproape tot ceea ce facem zi de zi este conectat la domeniul cibernetic prin echipamentele de comunicații moderne. Acest fenomen este rodul progresului tehnologic din sectorul industriei comunicației și tehnologiei informației.

Unul dintre pilonii acestei revoluții tehnologice este digitalizarea datelor și a informațiilor. În contextul prezentului studiu, digitalizarea reprezintă actul sau metoda prin care transformăm vocile, sunetele, muzica, culorile, imaginile, cuvintele, documentele și orice altă informație în biți, ca mai apoi să poată fi transferați în noua lor formă, electronică, cu ajutorul unui echipament modern de comunicații, precum este telefonul inteligent, prin undele radio, liniile de cupru, sateliți și magistralele de fibră optică, oriunde în jurul lumii, pe raze de mii de kilometri, în decurs de câteva fracțiuni de secundă. Acest rezultat extraordinar al modernizării, al progresului tehnologic, „digitalizarea”, este un element central și necesar procesului de

înțelegere a acestei noi ere, a globalizării.[1] Astfel, putem spune că democratizarea tehnologiei este promotorul globalizării producției.[2] Afirm asta deoarece unul din lucrurile urmărite în acest studiu de caz este nivelul și implicațiile aduse de utilizarea tehnologiilor (*hardware și software*) moderne asupra vieții personale, sociale și profesionale a populației din România anilor 2016-2018.

Pentru a putea face o afirmație în contextul unei cercetări științifice și într-o mai mare măsură în contextul securității naționale este nevoie de un fond de cunoștințe de la care să pornești o discuție și pe baza cărora să-ți argumentezi expunerea.

Deși nu este des întâlnită o astfel de abordare, studiul de caz aplicat populației rezidente din România ne oferă un excelent punct de pornire pentru acest demers.

După cum spune Sun Tzu, *„cunoaște-ți inamicul şi cunoaște-te pe tine însuți; într-o sută de bătălii nu te vei expune nici unei primejdii. Când nu-ți cunoști inamicul, dar te cunoști pe tine însuți, șansele tale de victorie sau de înfrângere sunt egale*."[3] Așadar, cunoașterea capacităților de securitate națională ale statului nostru și cunoașterea resurselor și intereselor actorilor statali și non statali adverși care pot aducere atingere intereselor României sunt o realitate care trebuie evidențiată mereu, devine aproape un truism.

În ceea ce privește studiul de caz dezvoltat în acest capitol, bazându-ne pe studiul literaturii de specialitate și a inițiativelor, respectiv pe proiectele statistice desfășurate la nivel european sau național cu privire la nivelul competențelor digitale și cultura de securitate digitală a populației din România, putem confirma faptul că nu am identificat o evaluare obiectivă și concludentă a culturii de securitate cibernetică. La nivel european există inițiative prin care se dorește

---

1. Thomas L. Friedman, *The Lexus and the Olive Tree – Understanding Globalization*, Ediția revizuită, Edit. Farrar, Straus and Giroux, New Yok, SUA, 2000, pp.46-47.
2. *Ibidem*, p.49.
3. Sun Tzu, *Arta Războilui* (trad. Alexandra Novaru, Raluca Pârvu), Edit. Imprimeria CORESI, Bucureşti, p.28.

o cunoaștere a nivelului de competențe digitale, precum este cazul proiectului „*The Digital Competence Wheel*"[1], cel al Comisiei Europene - „*DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*"[2] sau conform indicatorilor de performanță și ai documentației întocmite pentru Agenda Digitală Europeană 2009-2017[3]. În România, până în acest moment, s-a pus accent pe diverse studii teoretice și analizarea conceptelor ce fac referire la competențele digitale, precum sunt: diviziunea digitală, e-incluziune, inegalitatea digitală[4] șamd.

Pentru a răspunde coerent și consecvent la problemele trasate cu ocazia stabilirii obiectivelor de cercetare, voi evidenția perspective reale și abordabile în ceea ce privește guvernanța securității naționale prin management a securității spațiului virtual.

Pentru a îndeplini cerințele de cercetare privind atingerea obiectivul general, am considerat ca fiind importantă obținerea unor rezultate concrete prin răspunderea la întrebările de cercetare. Acest capitol va încerca să răspundă în mod special la cea de-a patra întrebare de cercetare[5], care privește contextul și nivelul culturii de securitate cibernetică a populației din România raportat la posibilitatea existenței unei interdependențe între nivelul culturii de securitate a utilizatorilor din România și impactul avut de acțiunile acestora

1. Anders Skov, The Center for Digital Generation, Digital Dannelse, „*The Digital Competence Wheel*", Copenhaga, 2016, https://digital-competence.eu/front/what-is-digital-competence/, accesat în data de 01.04.2019.
2. Carretero Gomez Stephanie, Vuorikari Riina, Punie Yves, Joint Research Centre, „*DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*", Ed. Publications Office of the European Union, Luxembourg, 2017.
3. Comisia Europeană, „Digital Single Market: European Broadband Markets", https://ec.europa.eu/digital-single-market/en/download-scoreboard-reports, accesat în data de 01.04.2019.
4. Laura Tufă, „Diviziunea digitală. Accesul şi utilizarea internetului în România, comparativ cu ţările Uniunii Europene", în *Calitatea Vieţii-Revistă de politici sociale*, anul XXI, nr. 1-2, Editura Academiei Române, București, 2010, pp.71-86.
5. Întrebarea nr.4. *Care este contextul și nivelul culturii de securitate cibernetică a populației din România?*

asupra dimensiunii securității cibernetice ca subdomeniu al securității naționale. Răspunsul la această întrebare poate aduce lumină în validarea sau invalidarea ipotezei secundare de cercetare și atingerea în parte a primului[1] și celui de-al doilea[2] obiectiv de cercetare al tezei. În acest sens, sub o atentă coordonare științifică, autorul întocmește un chestionar care odată aplicat este menit să ofere informații relevante privind cunoașterea și pregătirea eșantionului de persoane chestionate în vederea cuantificării unui grad de risc și impact asupra sistemului de securitate națională în România.

În cele ce urmează se va descrie metodologic și tehnic întregul proces de aplicare a chestionarelor și de obținere a rezultatelor care au fost analizate din punct de vedere statistic cantitativ și calitativ.

VI.1. Analiza statistică

Analiza statistică asupra culturii de securitate cibernetică a populației rezidente în România s-a obținut și din surse deschise de informații. Desigur, astfel de analize pot fi întocmite prin colectarea, evaluarea, verificarea și centralizarea datelor din comunicările și rapoartele emise de producătorii și furnizorii de soluții de securitate cibernetică, de CERT-RO, de Institutul Național de Statistică și de alte organisme naționale sau internaționale, dar nu în ultimul rând de cercetările de nișă orientate pe furnizarea de evaluări statistice și expunerea sau soluționarea problematicilor de securitate în general. Drept urmare, raportându-ne la ultimul Breviar Statistic al INS din 2018, putem observa că în cadrul lucrării de față ne raportăm la un eșantion final

1. Obiectiv nr.1. *Identificarea implicațiilor aduse de buna guvernanță a securității sectorului cibernetic ca parte integrantă a securității naționale pentru România în calitate de stat membru al Uniunii Europene.*
2. Obiectiv nr.2. *Identificarea determinantelor guvernanței securității naționale rezultate în urma adaptării sistemului de management al securității informației în spațiul virtual românesc.*

de 5.446 persoane din totalul de ~7.600 chestionare, care reprezintă ~0.03% din 19.644.350[1] persoane, care este numărul estimat al populației rezidente în România anului 2017.

VI.2. Identificarea necesității de conștientizare și protecție a societății contemporane în raport cu provocările cibernetice actuale și viitoare

Odată cu dezvoltarea posibilităților de comunicare a apărut posibilitatea multiplicării informației, ceea ce este pe de-o parte un real avantaj pentru întreaga societate, dar identificăm un dezavantaj care afectează din ce în ce mai mult credibilitatea surselor, anume mecanismele de dezinformare și adesea propagandă. Datorită existenței acestui pericol în mediul virtual, am apelat prin ANSSI la sisteme verificate de monitorizare și sinteză a presei[2] pe tematica securității cibernetice în plan național și european. Majoritatea informațiilor au fost verificate din cel puțin 4-5 surse distincte, acestea fiind atent analizate pentru a formula în final un argument. Puterea de analiză nu a stat în capacitatea automatismelor de sintetizare a știrilor, ci în analiza personală a acestor informații pe surse și în unele cazuri pe o contraverificare a rezultatelor cu specialiștii din acele domenii specifice de expertiză.

Deoarece am identificat un trend ascendent al evenimentelor și incidentelor din sectorul cibernetic privind sectorul public și cel privat, am decis să mă aplec asupra analizei cauzelor acestor problematici, întrucât tratarea efectelor nu a reprezentat niciodată o soluție reală pe termen lung.

1. Breviar Statistic, România în cifre, Institutul Național de Statistică, INS 2018, p.9, http://www.insse.ro/cms/sites/default/files/field/publicatii/romania_in_cifre_breviar_statistic_1.pdf, accesat în data de 01.04.2019.
2. Sistem de monitorizare a presei *online, social media, presa tipărită, radio și tv*, http://portal.klarmedia.com/.

VI.3. Chestionarul de evaluare a nivelului culturii de securitate cibernetică în România

Pornim de la considerentul că o evaluare reală, fidelă și granulară a nivelului culturii de securitate cibernetică în România nu poate să fie generată doar de aplicarea unor interviuri în rândul elitelor (*experți, specialiști, analiști, profesori, consultanți, șamd.*) care activează în sectorul securității cibernetice sau a decidenților, ori a instituțiilor de profil din sectorul public/privat. O astfel de abordare probabil ar genera o evaluare a nivelului de profesionalism raportat la persoanele evaluate în raport cu poziționarea pe *„piață”* a organizațiilor din care acestea fac parte, dar sub nici o formă nu ar oglindi nivelul de cultură de securitate.

A. Conceperea chestionarului

Motivat fiind de considerentele expuse mai sus și de necesitatea de a răspunde întrebărilor de cercetare propuse, am considerat potrivită aplicarea metodei chestionarului. Chestionarul din Anexa nr.1 este rezultatul a trei etape de validare. Toate cele trei forme au fost supuse analizei într-o comisie de specialitate. Persoanele identificate în această comisie au fost alese pe principiul expertizei în domeniul specialităților practicate de aceștia, anume un sociolog, un psiholog, un expert în securitate națională și a un expert în studiile statistice.

B. Validarea chestionarului

Pentru a-l putea valida și pentru a-i putea da o formă, chestionarul a fost aplicat unui număr de zece specialiști din sectorul tehnologiei informației și a comunicațiilor. Aceștia, unanim, au sugerat ca fiind necesară introducerea de întrebări concrete și suficient de tehnice cu privire la nivelul de cunoștințe în domeniul IT&C pentru a se putea evalua nivelul de cunoaștere a tehnologiei de comunicare și gestionare a informației în mediul virtual.

O a doua formă a fost dată după ce a fost aplicat un alt set de 10 chestionare experților din sectorul legislativ, care au evidențiat fap-

tul că este necesară o accentuare a aspectelor privind criminalitatea cibernetică, identificate tot mai des în sectorul economic virtual și nu numai.

Cea de-a treia etapă de actualizare și validare a întrebărilor chestionarului a fost marcată de evaluarea din punct de vedere statistic, etapă care a fost desfășurată sub atenta supraveghere a Departamentului Psihometrie și Statistică din cadrul Facultății de Științe Comportamentale și Sociale a Universității Groningen, cu ajutorul resurselor cărora am și finalizat studiul statistic al chestionarelor aplicate și care m-au orientat pas cu pas până la finalizarea studiului statistic. Experiența personalului din cadrul Universității Groningen cu care am intrat în contact și am lucrat m-a ajutat la obținerea de date statistice verificate și reverificate cu ajutorul instrumentelor utilizate de aceștia în zona de cercetare statistică cantitativă. Ulterior acestui proces, am obținut sprijinul colegilor din cadrul Departamentului Psihometrie și Statistică din cadrul aceleiași universități pentru o interpretare cât mai fidelă a datelor.

C. Aplicarea chestionarului

Odată cu alegerea temei de cercetare s-a identificat necesitatea valorificării unor date statistice care nu puteau fi obținute decât prin construirea și aplicarea unui chestionar. Acest instrument a avut ca unitate de eșantionare individuală populația finită, reală și cuantificabilă a României conform INS din perioada de colectare a datelor.

În acest context, eșantionul reprezintă utilizatorii români de echipamente moderne de comunicații și tehnologia informației în interes personal sau profesional. Așadar extrapolăm conceptul de *„eșantion"* ca populație țintă atent selecționată pentru aplicarea chestionarelor la întreaga *„populație"* cu abilități de utilizare a spațiului cibernetic, fără a restrânge eșantionul la limite de vârstă, sex, statut social, șamd.

A fost analizată și validată reprezentativitatea eșantionului ca o condiție de bază a validității externe și care depinde de cei patru factori luați în calcul la generarea întrebărilor chestionarului, anume:

caracteristica măsurată, impactul unor variabile covariante - date de relevanța rezultatelor întrebărilor, mărimea eșantionului[1] și procedura de eșantionare.

Receptivitatea și necesitatea acestui studiu a fost dovedită încă din momentul aplicării primelor 100 de chestionare, în acea perioadă s-a întâmpinat o receptivitate crescută în rândul persoanelor intervievate pentru a răspunde chestionarului și chiar de a dezvolta răspunsurile pentru o înțelegere mai bună a motivației răspunsului. Cu toate acestea, pe de-o parte datorită erorii de eșantionare, iar pe de altă parte a erorii în răspuns sau din lipsa acestora, din numărul total de 7.600 chestionare aplicate, un număr de 5.446 chestionare a fost validat, din care a fost acceptat în finalizarea raportului cantitativ un număr de 5.141 chestionare.

S-a utilizat tehnica de eșantionare probabilistă (aleatorie simplă) la o dimensiune a eșantionului pentru studii de validitate de construct foarte mare *(>1500 persoane*).

D. Centralizarea chestionarelor

Această etapă a fost cea mai solicitantă, motiv pentru care centralizarea datelor din chestionarele aplicate s-a întins pe o perioadă de aproximativ patru luni. În primele trei luni au fost introduse datele din chestionarele aplicate, care au fost în format scris pe hârtie. Din motive de autenticitate și veridicitate a datelor utilizate în acest studiu, chestionare originale sunt păstrate pentru o perioadă nedeterminată de timp.

E. Analiza statistică

Într-o ordine firească a lucrurilor, după centralizarea datelor a urmat etapa de pregătire pentru analiza și utilizarea acestora în

1. M. Popa – APIO, *Metodologia cercetării (note de curs)*: *„Cu cât eșantionul este mai mare, cu atât crește reprezentativitatea acesuia în rezultatele statistice. Nivelul de reprezentativitate nu va crește proporțional cu volumul eșantionului. Odată atins un volum de 700-800 de persoane, reprezentativitatea eșantionului nu mai crește semnificativ, indiferent de volumul populației din care este extras” (Rotariu, 1999), http://www.apio.ro/upload/mc10_esantionarea.pdf,* pp.2-8, accesat în data de 02.09.2020.

analiza statistică. Această analiză este de fapt secțiunea de analiză cantitativă în plan analitic din raportul studiului, regăsit în conținutul subcapitolului următor.

Predominant, analiza cantitativă a stat la bazele analizei calitative, utilizând în acest timp literatura de specialitate și aplicațiile informatice specializate în acest sens. În ceea ce privește interpretarea datelor pentru obținerea unui rezultat concludent în analiza calitativă, studiul și experiența acumulată pe parcursul celor trei ani au oferit rezultatul scontat, prin înțelegerea gradului de cultură de securitate pe care populația rezidentă în România îl are. De menționat, în ceea ce privește întrebările de cercetare ale tezei, în acest context este faptul că această analiză reprezintă o nouă posibilitate de cercetare a unui areal de interes major și obținerea unui indicator vital pe *„barometrul”* culturii de securitate cibernetică și desigur a securității naționale.

VI.4. Plan analitic

Ulterior aplicării chestionarelor a urmat centralizarea acestor date, pregătirea pentru analiza și utilizarea acestora în analiza statistică. Acest proces a presupus identificarea și excluderea cazurilor duplicate din baza de date, identificarea și excluderea cazurilor ce conțin răspunsuri logic imposibile sau improbabile (*de exemplu utilizatori care au declarat că au vârsta de 0 ani sau că petrec mai mult de 24 ore pe zi utilizând tehnologia digitală*), identificarea și excluderea răspunsurilor participanților cu vârsta prea mică *(mai mică de 14 ani*) sau prea mare *(mai mare de 70 ani*) pentru scopul acestui studiu și identificarea, respectiv excluderea cazurilor cu rate ridicate de răspunsuri lipsă (*de exemplu cazurile cu răspuns lipsă pentru mai mult de 80% din întrebări*).

Pentru a putea analiza datele în mod consecvent, utilizând același test statistic pentru analiza răspunsurilor la toate întrebările, variabila numerică *„vârsta”* a fost transformată în variabilă categorială. În acest

sens, utilizatorii cu vârsta sub 20 de ani au fost catalogați drept *„tineri”*, cei cu vârsta între 20 și 60 de ani au fost catalogați drept *„adulți”*, iar cei cu vârsta peste 60 de ani au fost catalogați drept *„vârstnici”*.

Deoarece aproape toate întrebările din chestionarul utilizat au generat date categoriale de tip nominal prin răspunsuri de tipul *DA/NU* sau de tip ordinal și scalabil (*de exemplu evaluarea importanței securității informatice pe o scală de la 1 la 5*), principala strategie analitică pe care am utilizat-o a fost analiza frecvențelor. Scopul a fost acela de a determina dacă există diferențe semnificative între participanți în ceea ce privește variabilele de interes din acest studiu, un exemplu ar fi cel în care cuantificăm măsura în care utilizatorii români consideră tehnologia digitală ca fiind importantă. De asemenea, ne-am propus să determinăm dacă există asocieri între anumite aspecte evaluate în cadrul acestui studiu, precum măsura în care utilizatorii au fost victime ale unor infracțiuni informatice în raport cu anumite aspecte ce țin de securitatea informatică.

Testul statistic potrivit pentru analiza frecvențelor este așa-numitul test *hi-pătrat, Pearson* χ^2 [1]. Acest test statistic poate fi utilizat pentru a determina dacă există diferențe semnificative statistic între frecvențele observate și cele teoretice (așteptate) în cadrul uneia sau a mai multor categorii de răspuns. Formula de calcul pentru χ^2 este:

$$\chi^2 = \sum \frac{(O-T)^2}{T},$$

unde *O* se referă la frecvențele observate, iar *T* se referă la frecvențele teoretice dintr-o categorie de răspuns sau dintr-o celulă a unui tabel de contingență (*sau tabel cu dublă intrare*). Aceste diferențe ridicate la pătrat se însumează pentru toate categoriile de răspuns (*în cazul testului* χ^2 *al gradului de omogenitate*) sau pentru toate celulele tabelului de contingență (*în cazul testului* χ^2 *al gradului de independență*).

1. Richard G. Lomax, Debbie L. Hahs-Vaughn, *Statistical concepts: A second course* - Ediția a 4-a, Edit. Routledge, New York, 2012 – Ediția a 4-a, Ed. Routledge, 2012, SUA, New York, Capitolul 8: „Multiple Regression, „Statistical concepts: A second course”.

În funcție de scopul analizei, χ^2 se poate utiliza pentru a determina dacă răspunsurile participanților se distribuie în mod egal între alternativele de răspuns (*testul* χ^2 *al gradului de omogenitate*) și dacă răspunsurile participanților la o anumită întrebare sunt independente de răspunsurile acestora la o altă întrebare (*testul* χ^2 *al gradului de independență*).

Un rol important în determinarea semnificației statistice a valorii χ^2 obținute îl au așa-numitele *grade de libertate*. Pentru testul χ^2 al gradului de omogenitate, acestea se calculează după formula *(r-1)*, unde *r* reprezintă numărul alternativelor de răspuns aferente unei întrebări. În cazul testului χ^2 al gradului de independență, gradele de libertate se calculează după formula *(r-1)×(c-1)*, unde *r* și *c* reprezintă numărul alternativelor de răspuns aferente celor două întrebări. În general, numărul gradelor de libertate se raportează imediat lângă χ^2, în paranteză *(ex.,* χ^2 *(1) = …).* Valoarea lui χ^2 și numărul gradelor de libertate se utilizează în calculul valorii *p*, valoare care, raportată la un prag critic (*de obicei 0.05, care înseamnă în analiza statistică și în cercetare în general o eroare experimentală asumată sau eroare de tip 1 - fals pozitiv*), determină *semnificația statistică* a efectului testat. Astfel, atunci când $p < 0.05$ respingem ipoteza nulă (*a omogenității sau a independenței*) și concluzionăm că există diferențe semnificative statistic între proporțiile aferente opțiunilor de răspuns, sau că există o asociere semnificativă statistic între variabile. Atunci când $p > 0.05$ nu respingem ipoteza nulă și concluzionăm că nu avem dovezi suficiente pentru a susține ipoteza alternativă (*a diferențelor între alternativele de răspuns sau a asocierii între variabile*).

Testul χ^2 ne oferă informații doar despre prezența (*în cazul în care* $p < 0.05$) diferențelor între categorii sau a asocierii dintre două variabile, însă nu și despre magnitudinea sau intensitatea acestor efecte. Pentru a putea determina cât de mari sunt diferențele dintre alternativele de răspuns sau cât de puternică este relația de asociere dintre variabile, avem nevoie de măsuri specifice. O astfel de măsură

a mărimii efectului, care este cel mai frecvent utilizată și este potrivită pentru toate aplicațiile testului χ^2, este *Cramer's V*[1]. Acest indice se calculează astfel:

$$Cramer's\ V = \sqrt{\frac{\chi^2}{N \times gl^*}}$$

unde *N* reprezintă numărul total de participanți care au răspuns întrebării sau întrebărilor asupra căreia/cărora se realizează testarea, iar $gl^* = 1$ în cazul testului χ^2 al gradului de omogenitate și $gl^* = \min(r - 1, c - 1)$ în cazul testului χ^2 al gradului de independență. O valoare *Cramer's V* egală cu 0.1 indică un efect scăzut, o valoare egală cu 0.3 indică un efect mediu, iar o valoare egală cu 0.5 indică un efect ridicat, evidențiind astfel că aceste valori - 0.1; 0.3; 0.5 - sunt numite și valori de referință în general acceptate ca valori ale mărimii efectului diferenței între frecvențe). Valori ale mărimii efectului mai mici de 0.1 indică un efect neglijabil pentru majoritatea scopurilor practice[2]. În acest studiu, am raportat și interpretat doar efectele cu un *Cramer's V* ≥ 0.1. Am decis acest lucru deoarece, atunci când eșantionul este mare, așa cum este cazul și în acest studiu, chiar și efectele extrem de mici tind să devină semnificative statistic.

Un alt indice util al mărimii efectului este așa-numitul *risc relativ*[3], care se aplică strict tabelelor de contingență 2×2. Acesta este definit ca raportul dintre incidența unui eveniment într-un anumit grup de persoane și incidența evenimentului într-un alt grup de persoane.

Fie tabelul de contingență:

1. Harald Cramér, *Mathematical Methods of Statistics*, Edit. Princeton University Press, Princeton, 1946, pp.10-14.
2. Jacob Cohen, „A power primer", în *Psychological Bulletin, Quantitative Methods in Psychology*, nr.112, Edit. American Psychological Association, Washington (DC), 1992, pp.155 -159;
3. Christopher L. Sistrom, Cynthia W. Garvan, „Proportions, odds, and risks", în *Statistical Concepts Series, Radiology*, Vol.230, Edit. University of Florida College of Medicine, Gainesville, 2004, pp.12-19;

	Predictor	
	Da	Nu
Da	A	B
Nu	C	D

Tabelul nr.2 - Tabel de contingență

Riscul relativ (RR) se calculează după formula:

$$RR = \frac{A/(A+C)}{B/(B+D)},$$

unde A, B, C și D reprezintă frecvențele observate. În acest studiu am folosit *RR* pentru a determina dacă anumite aspecte ce țin de securitatea informatică reprezintă sau nu factori de risc în favorizarea/ defavorizarea infracțiunilor informatice. Valori ale *RR* apropiate de 1 ar indica faptul că aspectele respective nu sunt asociate cu un risc crescut al utilizatorilor de a deveni victime ale infracțiunilor informatice. Pe parcurs ce valoarea *RR* crește, înțelegem că diferența față de valoarea 1 indica nivelul de incidență a respectivelor comportamente asociate unui risc crescut al utilizatorilor de a cădea victimă a infracțiunilor informatice. În aceeași ordine de idei, valori ale *RR* mult mai mici decât 1 indică faptul că respectivele comportamente reprezintă factori de securitate în raport cu riscul utilizatorilor de a cădea victimă a infracțiunilor informatice.

Toate analizele statistice au fost realizate în programele pentru analiză statistică R (*R programming language for statistical computing; R*[1] *Core Team, 2019 și SPSS*[2] *v.25.*

1. R Core Team (2019), „R: A language and environment for statistical computing", R Foundation for Statistical Computing, Vienna, Austria, URL: https://www.R-project.org/, accesat în data de 19.03.2019.
2. IBM Corp. (2017), „IBM SPSS Statistics for Windows - Statistical Package for Social Sciences", Version 25.0, Armonk, NY: IBM Corp, https://www-01.ibm.com/support/docview.wss?uid=swg24043678, accesat în data de 19.03.2019.

VI.4.1. Indici descriptivi ai eșantionului

Un număr de 5,446 persoane au participat la acest studiu în mod voluntar, la întâlniri programate, față în față, completând chestionarul. Răspunsurile a 52 participanți au fost eliminate din analiza finală a datelor, deoarece aceștia au declarat că au vârsta mai mică de 14 ani sau mai mare de 70 de ani. Așadar, pentru analiza finală a datelor au fost utilizate răspunsurile a unui număr de 5,141 participanți, reprezentând aproximativ 94% din eșantionul original. Dintre aceștia, 3,254 (63.3%) participanți au oferit răspunsuri complete la întrebările cu răspuns închis.

Analiza răspunsurilor incomplete arată că cele mai numeroase date lipsă (12.5% din totalul participanților) corespund întrebării *„Ați urmat vreodată cursuri în domeniul informatic?"*, urmată de întrebarea *"Ați fost vreodată victimă a unei infracțiuni informatice?"* cu 7.4% răspunsuri lipsă și de întrebarea *„Considerați că România este pregătită pentru un eventual val de atacuri cibernetice?"* cu 6.7% răspunsuri lipsă.

Distribuția participanților în funcție de gen a fost date de 53.8% participanți de gen feminin, 46.2% de gen masculin iar un număr de 1.5% nu au declarat apartenența de gen.

Vârsta participanților are o distribuție asimetrică spre dreapta, fiind reprezentată de o mediană egală cu 23 ani, iar 75% dintre participanți au sub 35 ani. Un procent de 2.2% dintre participanți nu și-au declarat vârsta.

În ceea ce privește mediul de proveniență al participanților, 29.3% dintre aceștia provin din mediul rural, iar 70.7% din mediul urban. Un procent de 6.6% dintre participanți nu și-au declarat mediul de proveniență.

Totodată, în funcție de statutul social, participanții se distribuie astfel: elevi și studenți în procente similare (45.0%, respectiv 41.9%), angajați și liber profesioniști în procente similare (5.3%. respectiv 5.2%), 2.6% șomeri și niciun pensionar. Un procent de 1.8% dintre participanți nu și-au declarat statutul social.

VI.4.2. Analiza competențelor digitale ale utilizatorilor români

Competențele digitale ale utilizatorilor români au fost evaluate printr-un set de 7 întrebări ce vizează aspecte precum nivelul competențelor digitale, tipul și scopul echipamentelor digitale utilizate, timpul petrecut utilizând tehnologia digitală, precum și importanța percepută cu privire la tehnologia digitală. Importanța percepției populației asupra utilizării mijloacelor moderne de comunicare și tehnologia informației conduce indirect la o evaluare a gradului de interes a utilizatorilor asupra securității propriilor date și informații vehiculate de aceștia în mediile virtuale precum și a echipamentelor utilizate. În alte cuvinte, gradul de percepție a importanței activităților din arealul cibernetic duce la un grad crescut sau scăzut de securitate a persoanei, a comunității și uneori a statului - *impactul negativ asupra statului sau a securității naționale poate fi cuantificat gradual (nesemnificativ - major) în funcție de rangul și influența persoanei care devine sursă generatoare de insecuritate*. Timpul petrecut utilizând tehnologia digitală este considerat un indicator, deoarece acesta este raportat la gradul de vulnerabilitate și riscurile asociate pe platformele online sau în utilizarea resurselor informatice. Desigur, acest timp de utilizare a tehnologiei oferă o perspectivă asupra gradul de expertiză și adaptabilitate la mediile virtuale, raportarea și chiar dependența de acesta.

S-a evaluat, de asemenea, măsura în care competențele digitale sunt asociate cu variabile socio-demografice precum genul, vârsta (tineri sub 20 ani, adulți între 20 și 60 ani, vârstnici peste 60 ani), mediul de proveniență (urban sau rural) și ocupația participanților (elev, student angajat, antreprenor / liber profesionist, sau șomer / fără ocupație). Rezultatele acestor analize sunt prezentate în următoarele paragrafe.

Deoarece majoritate breșelor de securitate sunt datorate fie lipsei de competențe digitale, fie de lipsa unei culturi de securitate, se

consideră oportună cunoașterea autopercepției utilizatorului în ceea ce privește nivelul său de competențe digitale. În cadrul întâlnirilor, după completarea chestionarului, adesea am pus întrebări de lămurire. Printre acestea se număra și *„Considerați că sunteți suficient de pregătit în ceea ce privește tehnologia utilizată?"*, iar răspunsurile erau de cele mai multe ori afirmative. Aceste întrebări de clarificare erau puse și cu scopul de a verifica încrucișat alte întrebări din conținutul chestionarului aplicat, precum *„Ați fost vreodată victimă a unei infracțiuni informatice*?" sau *„Aveți conturi online pe care le utilizați împreună cu altcineva?"*. De aici rezultă, adesea, faptul că nivelul de autopercepție asupra gradului de deținere a competențelor digitale sau nivelului culturii de securitate este eronat.

În ceea ce privește nivelul declarat al competențelor digitale ale participanților, mai mult de jumătate dintre aceștia dețin un nivel mediu de competențe, iar aproximativ o treime dețin un nivel ridicat (Figura nr.1).

Diferențele obținute pe eșantion pot fi generalizate la nivelul populației utilizatorilor din România, după cum arată testul χ^2, căruia îi corespunde un prag de semnificație mai mic de 0.05 ($\chi^2(2) = 1101.5$, $p < 0.01$). Din punct de vedere al mărimii efectului, aceste diferențe sunt medii (*Cramer's V* = 0.33). În ceea ce privește asocierea dintre nivelul de competențe al utilizatorilor români și variabilele socio-demografice, testele χ^2 ale gradului de independență au valori semnificative statistic pentru vârstă, mediu de proveniență și statut socio-economic, însă mărimile efectelor sunt foarte mici (*Cramer's V* < 0.1). Valori foarte mici ale mărimii efectului sugerează că asocierea dintre variabile este neglijabilă.

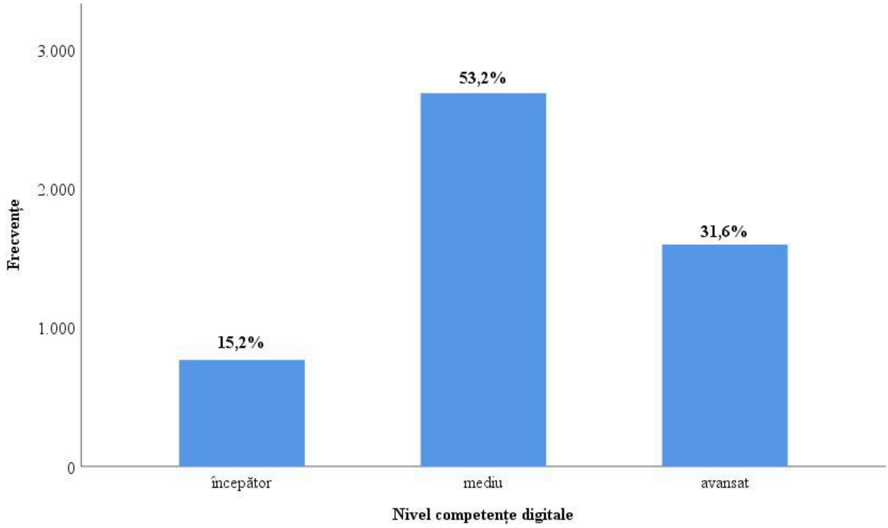


Figura nr.1. Distribuția participanților: Autopercepția corespondenților pe gradul de competențe digitale.

Procentele se bazează pe eșantionul efectiv (*i.e., numărul răspunsurilor valide*).

În ceea ce privește pregătirea formală în domeniul informatic, 42.5% dintre participanți au urmat cursuri de specializare, iar 57.5% dintre aceștia nu au urmat. Această diferență este semnificativă statistic ($\chi^2(1) = 102.5$, $p < 0.01$), însă efectul este scăzut (*Cramer's V* = 0.15). În ceea ce privește asocierea cu variabile socio-demografice, am găsit un rezultat semnificativ statistic și cu o valoare a mărimii efectului mică pentru asocierea cu statutul socio-economic ($\chi^2(4) = 65.4$, $p < 0.01$, *Cramer's V* = 0.12). Astfel, dintre cei care au urmat cursuri de formare în domeniu informatic, un procent ridicat sunt elevi (48.7%). De asemenea, semnificativ mai puțini sunt liber-profesioniștii (24.2%), șomerii sau persoanele fără ocupație (17.1%) care au urmat astfel de cursuri. Procentele răspunsurilor în fiecare categorie pot fi vizualizate în Figura nr.2. Mai mult, există o asociere moderată și semnificativă între nivelul competențelor digitale ale utilizatorilor români și dacă aceștia au urmat sau nu cursuri de pregătire în do-

meniul informatic ($\chi^2(2) = 448.7$, $p < 0.01$, *Cramer's V* = 0.32). Astfel, urmarea unor cursuri în domeniu informatic este asociată cu un nivel avansat al competențelor digitale: 49.0% dintre cei care au urmat astfel de cursuri dețin un nivel avansat al competențelor digitale.

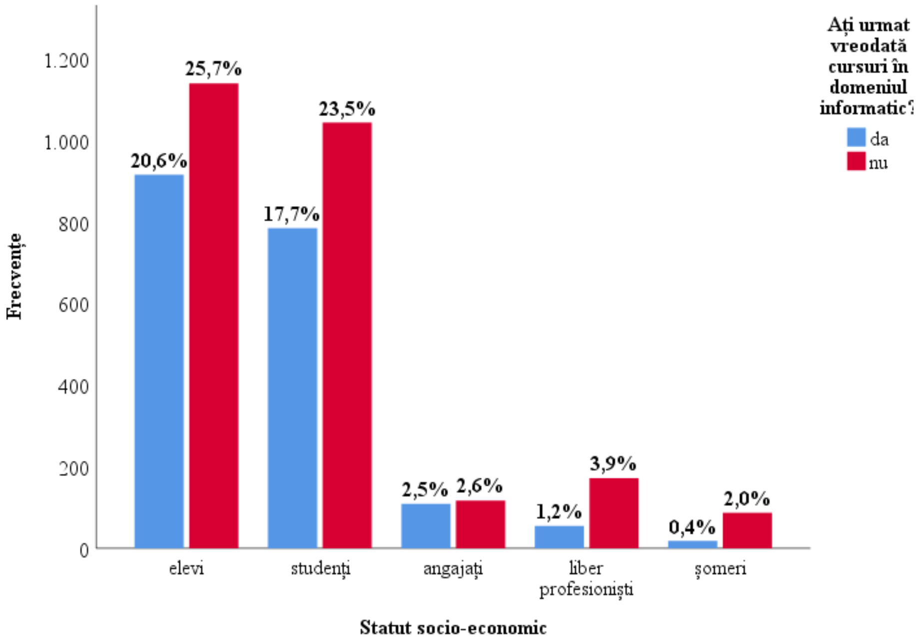


Figura nr.2. Distribuția participanților care au urmat cursuri în domeniu informatic și a celor care nu au urmat astfel de cursuri, separat în funcție de statutul socio-economic. Procentele au fost calculate din totalul răspunsurilor valide.

În ceea ce privește numărul de ore petrecute utilizând tehnologia digitală (Figura nr.3a), în medie utilizatorii din cadrul acestui eșantion fac acest lucru timp de 5 ore pe zi. Un sfert dintre participanți petrec mai puțin de 3 ore pe zi utilizând tehnologia digitală, în timp ce un sfert sunt online mai mult de 10 ore pe zi. Referitor la măsura în care acest timp este petrecut în mediul online (Figura nr.3b), datele arată că jumătate dintre respondenți petrec în mediul online între 50% și 100% din timpul dedicat utilizării tehnologiei digitale. Un sfert dintre respondenți petrec mai puțin de 50% din timp în mediul online, în

timp ce un sfert dintre ei petrec timpul dedicat tehnologiei digitale în mediul online în proporție de 100%.

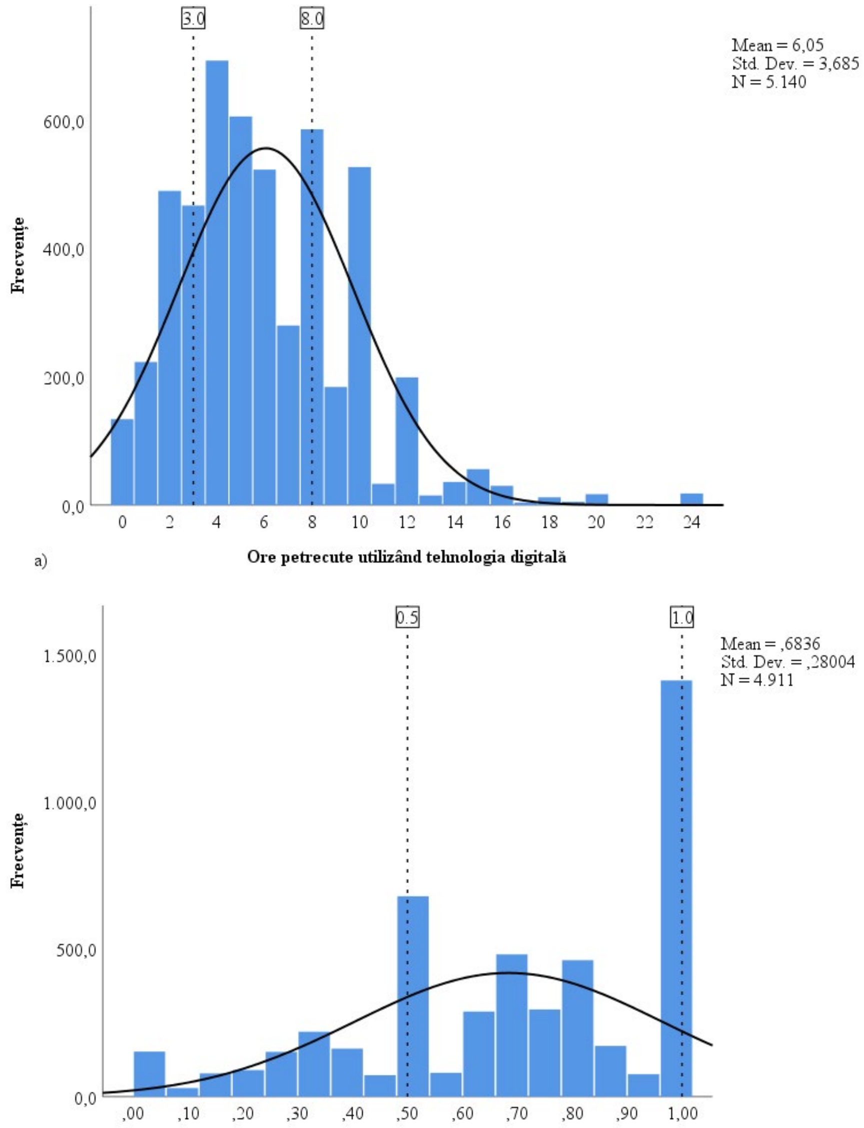


Figura nr.3. Distribuția numărului de ore petrecut utilizând tehnologia digitală (a) și a proporției din timp petrecut online (b). Liniile verticale corespund percentilelor 25 și 75[1].

1. *În cazul prezentului studiu, percentila 25 respectiv 75, se identifică cu procentul de persoane din eșantion care petrec până în 3 ore respectiv până în 8 ore pe zi, utilizând tehnologia*

Utilizarea aplicațiilor informatice este practicată în proporție de 90% de către utilizatorii români, diferența fiind semnificativă statistic și importantă din punct de vedere practic ($\chi^2(1) = 3371.1$, $p < 0.01$, *Cramer's V* = 0.81, care este o valoare mai mare de 0.5). Printre aplicațiile informatice menționate se numără Facebook, Microsoft Office, WhatsApp, Instagram, motoare de căutare online, sau diverse servicii de e-mail. Utilizarea acestor aplicații este statistic asociată cu vârsta utilizatorilor ($\chi^2(2) = 14.2$, $p < 0.01$, *Cramer's V* = 0.05) și cu statutul socio-economic al acestora ($\chi^2(4) = 21.8$, $p < 0.01$, *Cramer's V* = 0.07), însă aceste asocieri sunt neglijabile. Acest lucru sugerează că românii utilizează aplicațiile informatice în aceeași măsură indiferent de vârstă, mediu de proveniență sau statut socio-economic.

Referitor la importanța tehnologiei digitale pentru utilizatorii români, 31.3% dintre aceștia au declarat că tehnologia digitală este importantă pentru ei, 30.3% au declarat că aceasta este destul de importantă, iar 26.5% au declarat că aceasta este foarte importantă. Procentul de 11.8% rămas au declarat că pentru ei tehnologia digitală este puțin sau deloc importantă. Importanța percepută a tehnologiei digitale la români este asociată semnificativ statistic cu mediul de proveniență ($\chi^2(4) = 84.8$, $p < 0.01$, *Cramer's V* = 0.13) și statutul socio-economic ($\chi^2(16) = 548.8$, $p < 0.01$, *Cramer's V* = 0.17) al utilizatorilor. Utilizatorii care consideră tehnologia digitală ca fiind foarte importantă provin din mediul urban într-un procent mai ridicat (20.5%) decât ne-am fi așteptat în lipsa asocierii dintre variabile. A se consulta Figura nr.4 pentru vizualizarea distribuției răspunsurilor participanților în funcție de mediul de proveniență.

---

digitală.

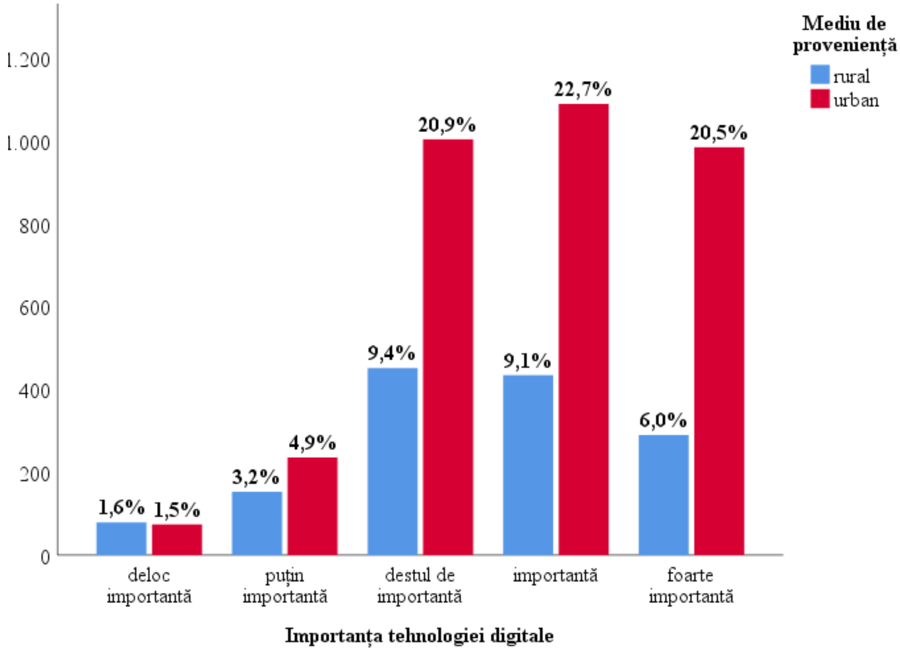


Figura nr.4. Distribuția importanței tehnologiei digitale în funcție de mediul de proveniență al participanților. Procentele afișate au fost calculate din totalul răspunsurilor valide.

Analiza corelației dintre importanța percepută a tehnologiei digitale și statutul socio-economic al utilizatorilor români arată că, dintre cei care consideră tehnologia digitală ca fiind deloc importantă, un procent mai ridicat decât ne-am fi așteptat în lipsa asocierii sunt șomeri sau liber profesioniști (23.2%). În ceea ce îi privește pe cei care consideră tehnologia digitală ca fiind puțin importantă, cei mai mulți utilizatori, mai mulți decât era de așteptat sunt șomeri sau liber profesioniști (26.7%). Pentru un număr mai mare de elevi decât ne-am fi așteptat (66.7%) tehnologia digitală este foarte importantă, iar 33.9% dintre studenți consideră tehnologia digitală ca fiind destul de importantă, un procent mai mare decât ne-am fi așteptat în lipsa asocierii dintre variabile. Cu alte cuvinte, observăm că importanța percepută a tehnologiei digitale diferă în funcție de statutul socio-economic al utilizatorilor. Astfel, elevii sunt cei mai mulți care

conferă o importanță ridicată sau foarte ridicată tehnologiei digitale, în timp ce mai mulți liber profesioniști și șomeri decât ne-am fi așteptat o consideră ca fiind puțin sau deloc importantă. Surprinzător este faptul că studenții consideră tehnologia digitală ca fiind foarte importantă într-un procent semnificativ mai mic (37.0%) și o consideră ca fiind puțin sau destul de importantă într-un procent mai ridicat (33.3%) decât era de așteptat. Interesant este și că în rândul angajaților nu există o tendință referitor la importanța percepută a tehnologiei digitale, întrucât răspunsurile acestora sunt omogene. Figura 5 ilustrează distribuția răspunsurilor participanților în funcție de statutul socio-economic

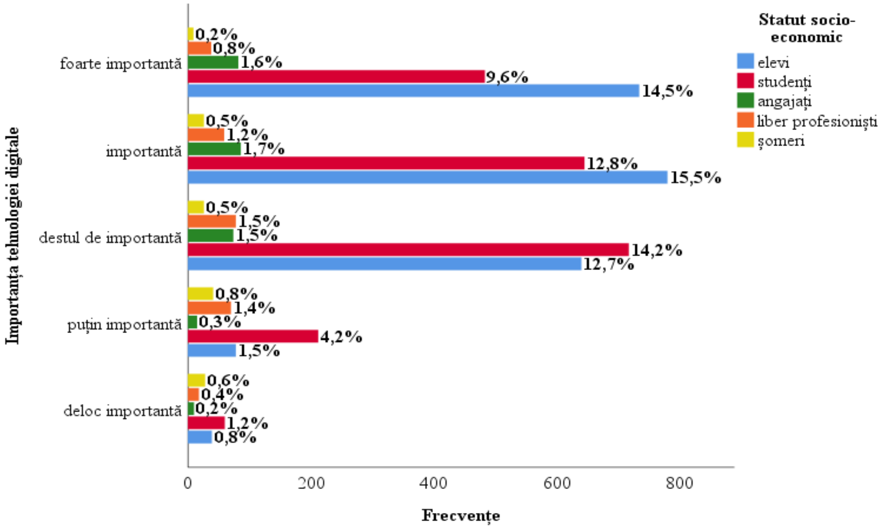


Figura nr.5. Distribuția importanței tehnologiei digitale în funcție de statutul socio-economic al participanților. Procentele au fost calculate din totalul răspunsurilor valide.

Referitor la tipul echipamentelor digitale utilizate, cel mai utilizat echipament este „*smartphone*"-ul, corespunzându-i un procent de 31.5% din totalul răspunsurilor și fiind folosit de 83.3% dintre participanți. Acesta este urmat de laptop și calculator (PC), cu 28.6% și 22.2% din totalul răspunsurilor. Astfel, 75.7% respectiv 58.7% dintre

participanți utilizează laptopul și PC-ul. Tableta este utilizată cel mai puțin (15.7% din totalul răspunsurilor), un procent de 41.7% dintre utilizatori folosind acest echipament. Un procent de 5.5% dintre utilizatori folosesc și alte echipamente, precum ceasurile inteligente, „*smart TV*"-urile, dronele, sau aparatele foto/video digitale. Tabelul nr. 1 prezintă procentul în care diverse echipamente digitale sunt utilizate în funcție de variabilele socio-demografice. Datele arată că, în general, echipamentele digitale precum „*smartphone*"-ul, laptopul, PC-ul sau tableta sunt utilizate de către persoane de gen feminin și persoane de gen masculin în proporții asemănătoare, însă preponderent de către adulți sau tineri, elevi sau studenți și persoane ce provin din mediul urban.

Variabilă	**Categorie**	**PC**	**Laptop**	**Tabletă**	**Smartphone**	**Altele**
Gen	Feminin	50.3%	55.2%	54.5%	53.0%	52.0%
	Masculin	49.7%	44.8%	45.5%	47.0%	48.0%
Vârstă	Tineri	19.7%	23.0%	20.7%	22.8%	19.3%
	Adulți	78.9%	76.5%	78.7%	76.3%	77.7%
	Vârstnici	1.4%	0.5%	0.6%	0.8%	2.9%
Mediu de proveniență	Rural	26.8%	26.1%	23.6%	28.1%	25.2%
	Urban	73.2%	73.9%	76.4%	71.9%	74.8%
Statut social	Elevi	42.0%	52.1%	46.1%	49.0%	47.3%
	Studenți	46.6%	38.7%	43.8%	39.3%	35.6%
	Angajați	5.1%	5.5%	6.0%	5.5%	6.9%
	Liber profesioniști	4.1%	3.0%	3.5%	4.9%	5.8%
	Șomeri	2.0%	0.7%	0.6%	1.3%	4.4%

Tabelul nr.3. Procentele de utilizare ale echipamentelor digitale în funcție de variabilele socio-demografice. Procentele sunt calculate din totalul participanților din fiecare categorie de echipament digital.

În ceea ce privește scopul utilizării tehnologiilor digitale, corespondenții au subliniat faptul că scopul utilizării acestor tehnologii moderne este dat de dorința și nevoia de utilizare a mediilor de comunicare și canalelor de socializare contemporane, cu 21.5% din

totalul răspunsurilor și fiind ales de 80% dintre participanți. Monitorizând activitățile infracționale în mediul online din ultimii ani, am observat că vulnerabilizarea utilizatorilor de tehnologie modernă se face tocmai prin spargerea conturilor de utilizator pentru obținerea de informații și date confidențiale[1], personale și din păcate uneori chiar cu caracter clasificat.

Un procent de 70.5% dintre utilizatori folosesc echipamentele digitale în scop de relaxare/distracție, 67.6% le folosesc în scop informațional, 51.7% pentru corespondență, 50.8% le folosesc pentru achiziții sau servicii online, 48.1% le folosesc în scop profesional, iar 3.8% dintre participanți folosesc echipamentele digitale în alte scopuri. Tabelul nr. 2 prezintă procentul în care echipamente digitale sunt utilizate în diverse scopuri, în funcție de variabilele socio-demografice. Astfel, majoritatea categoriilor socio-economice și demografice utilizează echipamentele digitale preponderent în scop de socializare, relaxare/distracție, sau în scop informațional.

Vârstnicii mai utilizează tehnologia digitală în scop de corespondență, iar studenții și angajații fac acest lucru și în scop profesional și de corespondență.

Concluzionând această secțiune, analiza competențelor digitale ale utilizatorilor români arată că majoritatea dețin, pe baza acestui chestionar, un nivel autoperceput mediu de competențe digitale, iar o treime dețin un nivel autoperceput, ridicat. Mai puțin de jumătate dintre utilizatori au urmat vreodată un curs de formare în domeniul informatic, iar cei care au urmat astfel de cursuri sunt elevi și dețin competențe digitale mai ridicate comparativ cu cei care nu au făcut acest lucru. Cele mai utilizate tipuri de echipamente digitale sunt telefoanele inteligente cunoscute și ca „*smartphone*", tableta și calculatoarele personale tip desktop, acestea fiind folosite preponderent în

1. Teodora Marinescu, „Un grup de hackeri a spart conturile mai multor politicieni din Germania şi a publicat datele personale", 04.01.2019, https://www.mediafax.ro/externe/un-grup-de-hackeri-a-spart-conturile-mai-multor-politicieni-din-germania-si-a-publicat-datele-personale-17810355/foto, accesat în data de 12.03.2019.

scop de socializare, relaxare / distracție sau pentru uz informațional. Studenții și angajații folosesc tehnologia digitală și în scop profesional și de corespondență într-o măsură mai mare. În medie, românii petrec 5 ore pe zi utilizând tehnologia digitală. Un sfert din românii chestionați sunt activi online mai puțin de 3 ore pe zi, iar un sfert dintre aceștia fac acest lucru mai mult de 10 ore pe zi. Timpul alocat tehnologiilor digitale este petrecut preponderent în mediul online, iar majoritatea covârșitoare a românilor, utilizează aplicații informatice precum, Facebook, WhatsApp, Instagram, motoare de căutare online, aplicații de e-mail, Microsoft Office, șamd.

În ceea ce privește importanța percepută a tehnologiei digitale, utilizatorii din mediul rural, șomerii, liber-profesioniștii și studenții o consideră deloc sau puțin importantă, în timp ce elevii consideră tehnologia digitală ca fiind importantă sau foarte importantă, în proporții mai ridicate decât era de așteptat.

Variabilă	Categorie	Profesional	Informațional	Socializare	Achiziții/ Servicii online	Corespon-dență	Relaxare/ Divertisment	Altele
Gen	Feminin	48.3%	70.5%	82.1%	50.5%	52.8%	70.1%	4.0%
	Masculin	47.6%	64.7%	77.6%	51.5%	50.4%	71.1%	3.4%
Vârstă	Tineri	30.0%	72.8%	87.9%	49.2%	44.4%	79.5%	2.3%
	Adulți	53.1%	66.8%	78.2%	51.9%	53.6%	68.6%	4.2%
	Vârstnici	28.9%	35.5%	50.0%	14.5%	43.4%	47.4%	3.9%
Mediu de proveniență	Rural	40.9%	59.8%	77.2%	42.7%	43.0%	68.1%	3.7%
	Urban	50.6%	71.0%	80.6%	54.0%	54.7%	71.2%	3.5%
Statut social	Elevi	39.4%	77.8%	89.2%	56.2%	52.6%	77.3%	3.6%
	Studenți	61.5%	61.6%	73.5%	49.4%	53.0%	65.1%	3.4%
	Angajați	68.0%	66.2%	72.2%	55.6%	60.2%	65.0%	6.8%
	Liber profesioniști	9.4%	40.4%	72.9%	29.0%	29.0%	68.2%	3.5%
	Șomeri	13.0%	38.3%	47.8%	11.3%	40.0%	51.3%	7.0%

Tabelul nr.4. Distribuția scopului utilizării echipamentelor digitale în funcție de variabilele socio-demografice. Procentele sunt calculate din totalul participanților din fiecare categorie a variabilelor socio-demografice.

VI.5. Analiza culturii de securitate informațională a utilizatorilor din România

În România, printre singurele cercetări concludente cu privire la cultura de securitate în context cibernetic a fost *„Barometrului Culturii de Securitate”*, un proiect realizat de Institutul de Științe Politice și Relații Internaționale *„Ion I. C. Brătianu”* al Academiei Române și Laboratorul de Analiză a Războiului Informațional și Comunicare Strategică (*LARICS*). Acest barometru a fost conceput pentru a demistifica cultura politică în contextul culturii de securitate, componenta strategică a culturii de securitate, *în general* și controversatul binom cultura de securitate și războiul informațional. Acesta are un rol și rost care, analizat în ansamblu, oferă răspunsuri concrete la anumite contexte și situații discutate pe aria studiului de față.

Rezultatele acestui barometru sunt mai puțin specifice, acestea reglementând mai degrabă un mediu de securitate în care securitatea trebuie generată prin construirea unei culturi publice de securitate, o cultură a rezilienței democratice, *„iar sentimentul specific generat de o astfel de cultură este cel al predictibilității instituționale. Într-un ambient instituțional dominat de reziliență, emoțiile preponderente sunt pozitive, precum încredere, optimism, asertivitate. În al doilea rând, în cultura publică de securitate apar percepții colective legate de cine ne sunt inamicii, cum ne amenință aceștia și cum ne putem apăra eficient. Aceste percepții apar ca urmare a difuzării narațiunilor strategice ale elitei de tipul cine suntem noi și cum vrem să arate lumea noastră.*

Cultura de insecuritate este cultura rezilienței neo-patrimoniale. În matricele instituționale neo-patrimoniale, majoritatea cetățenilor împărtășesc emoții negative, respectiv sentimente de angoasă, pesimism și neîncredere în forțele proprii. Dincolo de abordarea ideal-tipică, în funcție de tipul de ambient instituțional și de datele socio-demografice ale respondenților, vom găsi în realitatea socială atât emoții specifice culturii de securitate, cât și emoții tipice pentru cultura de insecuritate. Pentru o măsurare cât mai

precisă a realității sociale se impune rafinarea permanentă a ideal-tipului culturii de securitate.

Cultura de securitate este o variabilă latentă, motiv pentru care nu se poate măsura direct. Este nevoie în acest sens de o serie de indicatori intermediari.

Cultura de securitate este un proces. Nu este o entitate transcendentă și monolitică. Este o construcție social-instituțională influențată de elemente de non-securitate locale și internaționale, precum și de procesul de socializare parcurs de un stat în organizațiile și instituțiile internaționale.

Cunoscând starea culturii de securitate, cunoaștem starea legitimității verticale și orizontale a statului, dar și emoțiile dominante în rândul unei populații."[1]

Am pus accentul pe necesitatea de reliefare în concret a unor aspecte care pot încadra conceptul de cultură de securitate informațională în rândul nevoilor principale ale utilizatorilor români activi în mediul online. În conținutul chestionarului s-au formulat întrebări specifice pentru a obține rezultate concrete în generarea unei posibile definiții a culturii de securitate informațională, care să fie corect raportată la realitatea fenomenului general și la percepția cetățenilor din Româna asupra conceptului de securitate cibernetică.

Cultura de securitate informațională a utilizatorilor români a fost analizată printr-un set de întrebări ce evaluează importanța percepută a securității informatice, comportamente concrete prin care transpare cultura de securitate informatică a utilizatorilor (*exemplificând prin deținerea de conturi online pe care le utilizează împreună cu altcineva sau reacția subiecților chestionarului la cazurile de infracțiune informatică sau breșe de securitate)*, măsura în care au fost victime ale infracțiunilor informatice sau măsura în care apropiați ai acestora au fost victime a

1. Lucian Dumitrescu, „Lansarea Barometrului Culturii de Securitate. Ce este Cultura de Securitate?", 12.04.2018, https://larics.ro/lansarea-barometrului-culturii-de-securitate-ce-este-cultura-de-securitate/, accesat în data de 22.07.2019.

infracțiunilor informatice, măsura în care participanții la studiu consideră că România este pregătită pentru un val de atacuri cibernetice și în baza răspunsurilor acestora - prin auto-evaluare -măsura în care consideră importantă introducerea studiului securității cibernetice în școli și universități - în sectorul de învățământ indiferent de ciclul de studii. De asemenea, am evaluat asocierea dintre aceste aspecte, pe de o parte, și variabilele socio-demografice, iar pe de altă parte am evaluat nivelul competențelor digitale.

Sumarul secțiunii: Majoritatea studenților, angajaților și utilizatorilor români cu competențe digitale avansate au auzit despre conceptul de securitate informatică, în timp ce mai mulți liber profesioniști, șomeri și persoane cu un nivel scăzut de competențe digitale nu cunosc acest concept. Totodată, cei mai mulți utilizatori români - *în special cei cu un nivel mediu sau avansat al competențelor digitale sau cei care au urmat cursuri de formare în domeniul informatic* - consideră că securitatea informatică este importantă sau foarte importantă. Cu toate acestea, aproape jumătate dintre ei se fac vulnerabili unor atacuri informatice prin unul sau mai multe comportamente de risc, cum sunt încredințarea datelor personale unor persoane străine, oferirea sau divulgarea documentelor personale, parolelor/conturilor de acces și/sau informațiilor cu caracter confidențial, sau includerea în lista de contacte a unor persoane necunoscute. În special elevii tind să întreprindă acțiuni prin care se fac vulnerabili atacurilor cibernetice. Cu o frecvență mai ridicată decât era de așteptat, aceștia subscriu unor cauze neverificate, utilizând adresa de e-mail, deschid mesajele prin care sunt anunțați că au câștigat un premiu fără să fi participat la vreun concurs sau tombolă, divulgă parole sau conturi de acces, sau dețin în lista lor de contacte persoane pe care nu le cunosc. Din totalul utilizatorilor, mai mult de o treime au în cercul de prieteni victime ale infracțiunilor informatice, iar aproape 20% au fost ei înșiși victime ale unor astfel de infracțiuni. Dintre aceștia, aproximativ două treimi au fost victimele infectării sistemelor informatice cu programe

malițioase, iar câte o treime au fost victimele furtului de date personale respectiv al furtului de identitate. Un risc crescut de a deveni victime prezintă cei care răspund mesajelor sau urmează instrucțiunile din mesajele care îi înștiințează că au câștigat un premiu fără să fi participat la vreun concurs, cei care divulgă documente personale, parole/conturi de acces sau informații cu caracter confidențial și cei care au în cercul de prieteni victime ale infracțiunilor informatice.

Majoritatea utilizatorilor români nu cred că România este pregătită pentru un val de atacuri informatice și consideră importantă și foarte importantă introducerea studiului securității informatice în mediul preuniversitar și universitar. În continuare prezentăm aceste rezultate în mod detaliat.

Întrebați dacă au auzit vreodată despre expresia *„securitate informatică"*, 67.6% dintre participanți au răspuns în mod afirmativ, iar diferența dintre proporții este medie și semnificativă statistic ($\chi^2(1) = 633.7$, $p < 0.01$, *Cramer's V* = 0.35). Printre definițiile oferite de participanți se numără răspunsuri precum: *„se referă la protecția datelor cu caracter personal"*, *„eliminarea riscurilor utilizării echipamentelor digitale, informatice"*, *„siguranța pe internet"* sau *„criptarea informației"*. Răspunsurile la această întrebare corelează într-o oarecare măsură cu statutul socio-economic al utilizatorilor ($\chi^2(4) = 167.4$, $p < 0.01$, *Cramer's V* = 0.18), cu nivelul competențelor digitale ale acestora ($\chi^2(2) = 306.5$, $p < 0.01$, *Cramer's V* = 0.25) și cu măsura în care au urmat cursuri de formare în domeniul informatic (da/nu; $\chi^2(1) = 161.9$, $p < 0.01$, *Cramer's V* = 0.19).

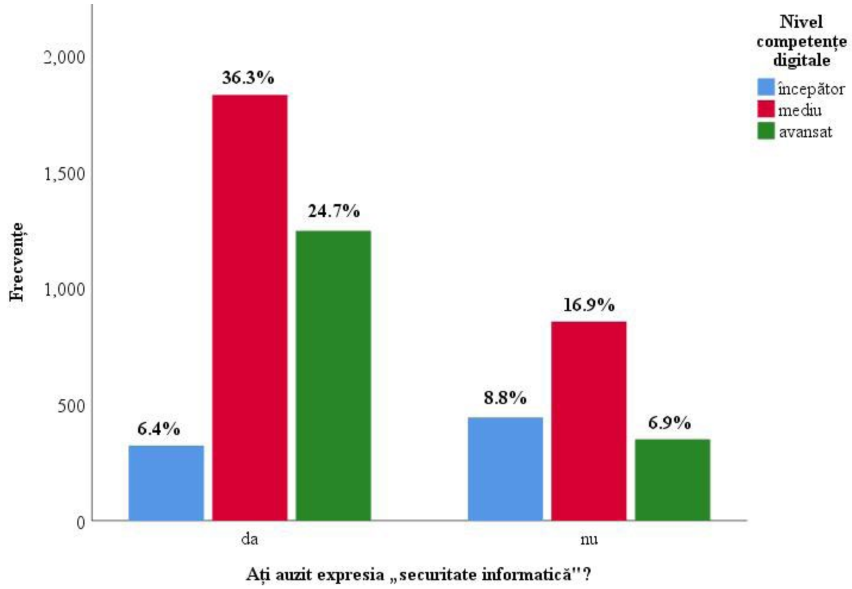


Figura nr.6. Distribuția utilizatorilor care au auzit și a celor care nu au auzit despre securitate informatică în funcție de statutul socio-economic al acestora. Procentele sunt calculate din totalul cazurilor valide.

Astfel, un număr mai mare de studenți (70.6% dintre aceștia), angajați (76.4% dintre aceștia) și utilizatori cu competențe digitale avansate (78.1% dintre aceștia) au auzit despre acest concept, în timp ce un număr mai mare de liber profesioniști (64.3% dintre aceștia), șomeri (53.9% dintre aceștia) și persoane cu un nivel scăzut de competențe digitale (57.9 dintre aceștia) nu au auzit niciodată despre acest concept (*distribuția răspunsurilor poate fi vizualizată în **Figura 6***).

Totodată, răspunsurile afirmative la această întrebare se asociază cu participarea la cursuri de formare în domeniul informatic, 78.6% dintre cei care au auzit despre conceptul de securitate informatică spunând că au urmat cursuri în domeniul informatic.

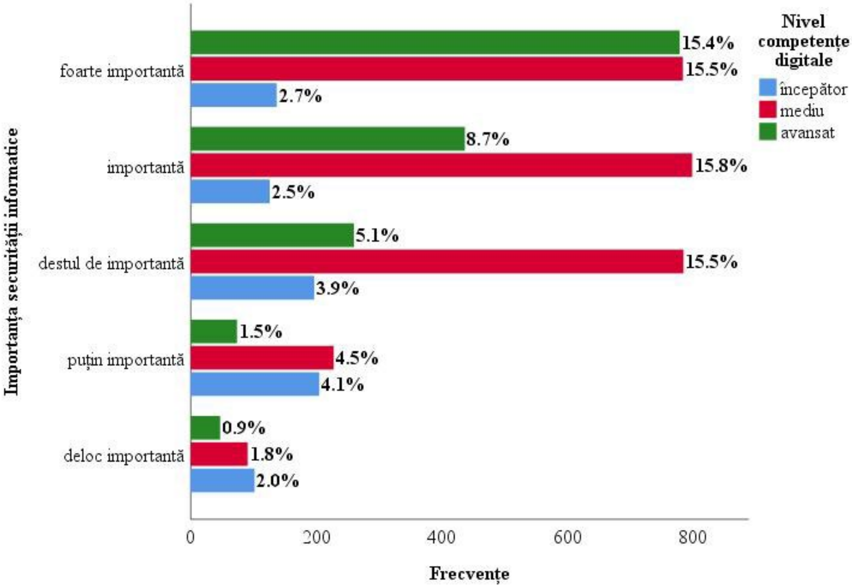


Figura nr.7. Distribuția importanței percepute a securității informatice în funcție de nivelul competențelor digitale ale utilizatorilor. Procentele sunt calculate din totalul cazurilor valide.

Referitor la importanța percepută a securității informatice pentru utilizatorii români, datele se distribuie astfel: pentru 60.1% dintre utilizatori securitatea informatică este importantă sau foarte importantă, pentru 24.4% aceasta este destul de importantă, iar pentru 15.4% dintre utilizatori securitatea informatică este puțin sau deloc importantă. Diferențele dintre categoriile de răspunsuri sunt semnificative statistic și au o magnitudine mică spre medie (*Cramer's V* = 0.26). Importanța percepută asupra securității informatice este asociată semnificativ statistic cu:

- genul, vârsta, mediul de proveniență, statutul socio-economic (*efecte neglijabile sau mici; Cramer's V < 0.1*);
- nivelul competențelor digitale ($\chi^2(8) = 694.5$, $p < 0.01$, *Cramer's V* = 0.26, Figura nr.7);
- participarea la cursuri de formare în domeniul informatic ($\chi^2(4) = 230.4$, $p < 0.01$, *Cramer's V* = 0.23).

Astfel, o importantă percepută ridicată sau foarte ridicată (categoriile *„importantă”* sau *„foarte importantă”*) a securității informatice se asociază cu un nivel mediu (29.7% dintre cei cu nivel mediu) sau avansat (48.8% dintre cei cu nivel avansat) al competențelor digitale, pe când o importanță scăzută (*„puțin importantă”*) sau foarte scăzută (*„deloc importantă”*) a securității informatice se asociază cu un nivel scăzut (40% dintre începători) al competențelor digitale. De asemenea, urmarea unor cursuri în domeniul informatic este asociat cu o percepție ridicată a importanței securității informatice (44.9% dintre cei care au urmat vreun curs în domeniul informatic consideră securitatea informatică ca fiind foarte importantă).

Referitor la acțiunile sau caracteristicile utilizatorilor români prin care transpare cultura de securitate informatică a acestora, prezentăm următoarele rezultate pe baza acestui eșantion: Semnificativ mai mulți utilizatori (70.5%; $\chi^2(1) = 837.6$, $p < 0.01$, *Cramer's* $V = 0.41$) declară că:

- nu au vorbit niciodată despre aspecte din viața lor personală cu persoane străine;
- nu au susținut diverse cauze (umanitare, șamd.) prin subscriere cu adresa de e-mail (61.0%; $\chi^2(1) = 340.1$, $p < 0.01$, *Cramer's* $V = 0.26$) sau cu sume de bani (59.3%; $\chi^2(1) = 170.3$, $p < 0.01$, *Cramer's* $V = 0.19$);
- nu au încredințat date personale unor persoane străine (54.7%; $\chi^2(1) = 44.0$, $p < 0.01$, *Cramer's* $V = 0.10$);
- nu au oferit de bunăvoie copii după documente personale (67.1%; $\chi^2(1) = 580.9$, $p < 0.01$, *Cramer's* $V = 0.34$);
- nu au cerut și nu li s-a solicitat vreodată ajutorul pentru utilizarea unui card bancar (57.8%; $\chi^2(1) = 122.9$, $p < 0.01$, *Cramer's* $V = 0.16$);
- nu au în lista de contacte persoane necunoscute (59.0%; %; $\chi^2(1) = 162.7$, $p < 0.01$, *Cramer's* $V = 0.18$);
- nu dețin conturi online pe care le utilizează împreună cu altcineva (82.5%; $\chi^2(1) = 2076.1$, $p < 0.01$, *Cramer's* $V = 0.65$).

Cu toate acestea, un procent de 46.1% dintre utilizatori au declarat că au oferit, prin constrângere, documente (67.7%), parole/conturi de acces (27.7%) și/sau informații cu caracter confidențial (29.4%).

Un procent de 57.8% din utilizatori au fost înștiințați, prin telefon sau e-mail că au câștigat un premiu/sumă de bani fără să fi participat la vreun concurs sau tombolă ($\chi^2(1) = 120.5$, $p < 0.01$, *Cramer's V* = 0.16). Dintre aceștia, 83.5% au deschis mesajul, 14.6% au răspuns mesajului, 8.1% au urmat instrucțiunile din mesaj, iar 13.8% au șters mesajul.

O parte din acțiunile și caracteristicile descrise anterior sunt asociate cu variabile socio-demografice și/sau cu importanța percepută a securității informatice a utilizatorilor. Astfel, susținerea unor cauze prin subscrierea cu adresa de e-mail este asociată cu statutul de elev (49.2%% dintre cei care subscriu), pe când mai puțini șomeri (*1.2%* dintre cei care subscriu) și liber-profesioniști (*3.5%* dintre cei care subscriu) fac acest lucru ($\chi^2(4) = 48.8$, $p < 0.01$, *Cramer's V* = 0.10). **Figura 8** ilustrează distribuția răspunsurilor utilizatorilor la acești doi itemi.

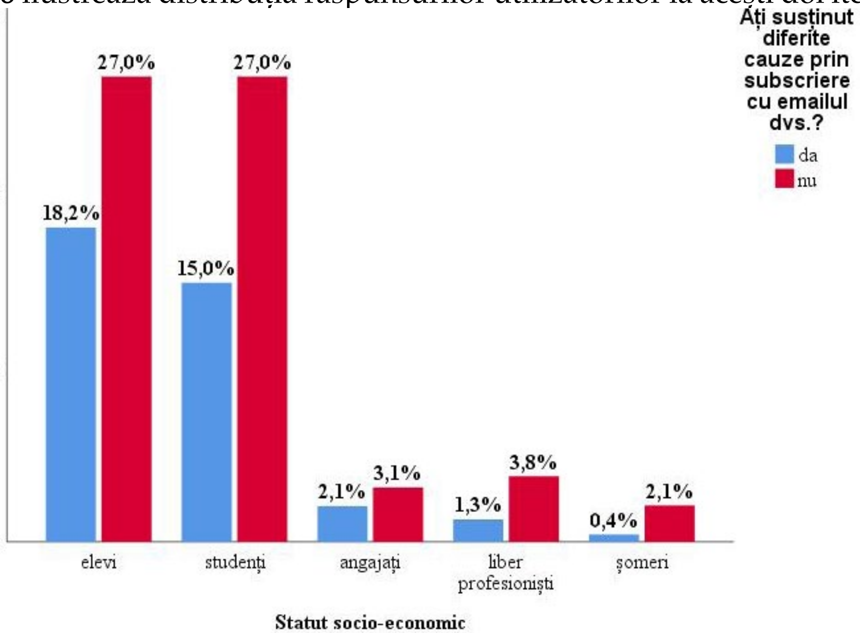


Figura nr.8. Distribuția celor care subscriu cu adresa de e-mail diferitelor cauze, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide.

Surprinzător, dintre cei care consideră securitatea informatică ca fiind foarte importantă, un număr mai mare decât ne-am fi așteptat (44.6%) subscriu diferitelor cauze utilizând adresa de e-mail ($\chi^2(4) = 95.7$, $p < 0.01$, *Cramer's V* = 0.14) sau declară că au primit mesaje nesolicitate prin telefon sau e-mail prin care au fost înștiințați că au câștigat un premiu sau o sumă de bani, fără să fi participat la vreo formă de concurs sau tombolă (65.3%; $\chi^2(4) = 98.8$, $p < 0.01$, *Cramer's V* = 0.14). Mai mult, dintre cei care primesc astfel de mesaje sau e-mailuri, un număr mai mare decât ne-am fi așteptat deschid aceste mesaje deși declară că pentru ei securitatea informatică este foarte importantă (49.4% dintre utilizatorii care conferă o importanță ridicată securității deschid mesajele primite; $\chi^2(4) = 76.4$, $p < 0.01$, *Cramer's V* = 0.12), ceea ce ne spune că pe deoparte ori nu înțeleg noțiunea de securitate informatică pe deplin ori duc la împlinire acțiuni fără a raționa efectele și riscurile la care aceștia se supun. Totodată, majoritatea celor care deschid acest tip de mesajele, sunt elevi (50.2%; $\chi^2(4) = 57.8$, $p < 0.01$, *Cramer's V* = 0.11; **Figura 9)**.

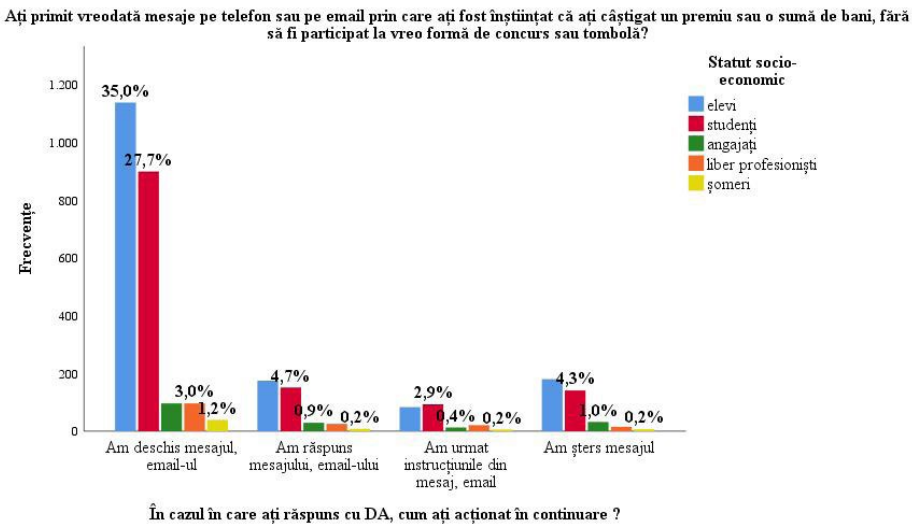


Figura nr.9. Distribuția celor care răspund mesajelor, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide.

Dintre cei care susțin campanii umanitare sau sociale cu sume mici de bani, un procent destul de mare este dat de studenți (45.9%) sau angajați (7.0%; $\chi^2(4) = 65.2$, $p < 0.01$, *Cramer's V* = 0.12] și care conferă o importanță ridicată sau foarte ridicată securității informatice (66.1%; $\chi^2(4) = 51.7$, $p < 0.01$, *Cramer's V* = 0.10). În ceea ce privește divulgarea prin constrângere a parolelor / conturilor de acces, elevii prezintă un risc mai ridicat la acest capitol ($\chi^2(4) = 73.9$, $p < 0.01$, *Cramer's V* = 0.12), un procent de 59.4% dintre cei care au declarat că au fost constrânși să divulge parole sau conturi de acces fiind elevi (Figura nr.10).

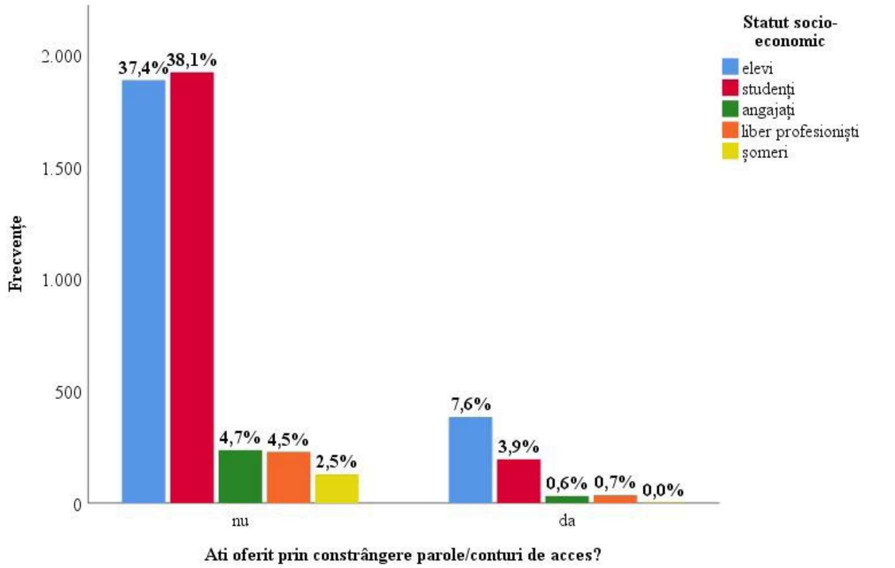


Figura nr.10. Distribuția celor care au divulgat prin constrângere parole sau conturi de acces, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide.

Mai mulți elevi (47.3% dintre elevi) și tineri până în 20 de ani (48.6% dintre tineri) decât ne-am fi așteptat au în lista lor de contacte persoane pe care nu le cunosc ($\chi^2(4) = 103.1$, $p < 0.01$, *Cramer's V* = 0.15 pentru asocierea cu statutul socio-economic; $\chi^2(2) = 57.7$, $p < 0.01$, *Cramer's V* = 0.11 pentru asocierea cu vârsta) (**Figura nr.11**).

Un procent de 36.6% dintre utilizatori au în cercul lor de prieteni persoane victime ale unor infracțiuni informatice, iar 17.8% dintre utilizatori au fost ei înșiși victime ale unor astfel de infracțiuni. Dintre aceștia din urmă, 66.6% au fost victimele infectării sistemului informatic cu aplicații și programe malițios intenționate, 35.2% au fost victimele furtului de date personale, iar 32.5% au fost victimele furtului de identitate.

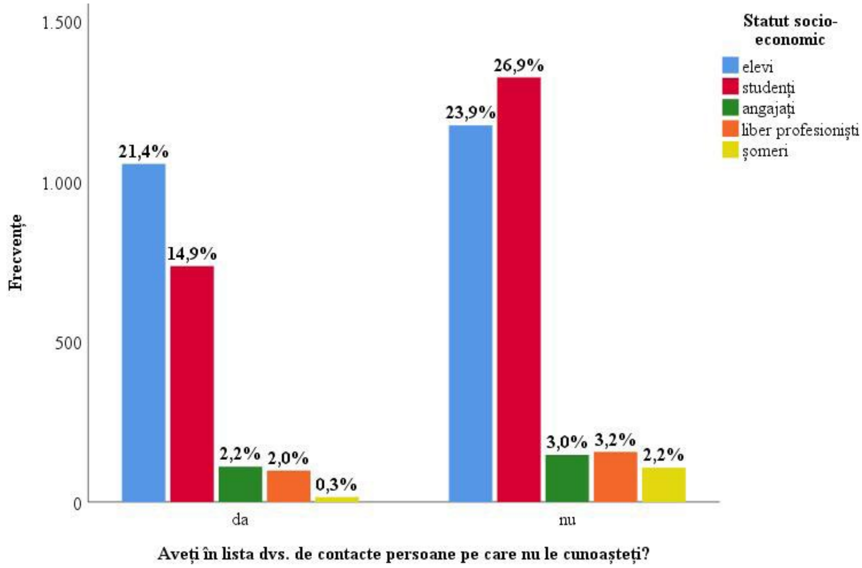


Figura nr.11. Distribuția celor care au în lista lor de contacte persoane pe care nu le cunosc, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide.

În general, un risc mai ridicat de a deveni victime ale infracțiunilor informatice prezintă utilizatorii care: au în cercul lor de prieteni persoane care au fost victime ale unor infracțiuni informatice (un risc de 4 ori mai mare; $\chi^2(1) = 484.8$, $p < 0.01$, *Cramer's* $V = 0.32$); împărtășesc aspecte din viața lor personală cu persoane necunoscute (cu un risc de 1.7 or mai ridicat; $\chi^2(1) = 74.1$, $p < 0.01$, *Cramer's* $V = 0.13$); încredințează date personale unor persoane străine (un risc de 1.6 ori mai mare; $\chi^2(1) = 47.4$, $p < 0.01$, *Cramer's* $V = 0.11$); oferă copii după

documente personale (un risc de 1.7 ori mai ridicat; $\chi^2(1) = 63.4$, $p < 0.01$, *Cramer's V* = 0.12); oferă sau solicită ajutorul pentru utilizarea unui card bancar (un risc de 1.7 ori mai mare; $\chi^2(1) = 52.2$, $p < 0.01$, *Cramer's V* = 0.11); dețin în lista de contacte persoane pe care nu le cunosc (un risc de 1.7 ori mai mare; $\chi^2(1) = 70.3$, $p < 0.01$, *Cramer's V* = 0.12); dețin conturi online pe care le utilizează cu altcineva (un risc de 1.7 ori mai mare; $\chi^2(1) = 67.0$, $p < 0.01$, *Cramer's V* = 0.12); primesc mesaje prin telefon sau e-mail că au câștigat un premiu sau sumă de bani fără să fi participat la vreun concurs sau tombolă (un risc de 1.8 ori mai ridicat; $\chi^2(1) = 70.0$, $p < 0.01$, *Cramer's V* = 0.12).

O analiză mai amănunțită a tipurilor de infracțiune informatică cărora utilizatorii le cad victime relevă următoarele:

A. un risc crescut de a cădea victime furtului de date personale îl prezintă utilizatorii care, atunci când sunt anunțați că au câștigat un premiu fără să fi participat la vreun concurs/ tombolă:
   - *răspund mesajelor (un risc de 6 ori mai mare; $\chi^2(1) = 340.5$, $p < 0.01$, Cramer's V = 0.26);*
   - *urmează instrucțiunile (un risc de aproape 10 ori mai mare; $\chi^2(1) = 565.2$, $p < 0.01$, Cramer's V = 0.33).*

B. au fost constrânși să divulge
   - *documente personale (un risc de aproape 3 ori mai mare; $\chi^2(1) = 86.9$, $p < 0.01$, Cramer's V = 0.13);*
   - *parole / conturi de acces (un risc de 4.5 ori mai mare; $\chi^2(1) = 226.1$, $p < 0.01$, Cramer's V = 0.21)*
   - *sau informații cu caracter confidențial (un risc de 3 ori mai mare; $\chi^2(1) = 116.7$, $p < 0.01$, Cramer's V = 0.15).*

C. Pentru furtul de identitate și virusarea sistemului informatic rezultatele sunt foarte similare cu cele aflate pentru furtul de date personale, în ceea ce privește riscul relativ și semnificația statistică a acestuia.

Întrebați dacă cred că România este pregătită pentru un eventual val de atacuri cibernetice, semnificativ mai mulți utilizatori au răspuns în mod negativ (63.9%; $\chi^2(1) = 367.7$, $p < 0.01$, *Cramer's V* = 0.28). Printre motivele enumerate de aceștia se numără lipsa specialiștilor și a pregătirii profesionale în acest domeniu, lipsa fondurilor și a infrastructurii necesare, instabilitatea sistemului informatic sau o informare slabă despre securitatea informatică. Dintre utilizatori, semnificativ mai mulți cred că este importantă sau foarte importantă introducerea studiului securității informatice în mediul preuniversitar (65.7% dintre utilizatori) și în mediul universitar (72.9% dintre utilizatori). Aceste răspunsuri sunt asociate semnificativ statistic cu o importanță percepută foarte ridicată a securității informatice, atât în ceea ce privește introducerea acestor studii în mediul preuniversitar ($\chi^2(16) = 1756.6$, $p < 0.01$, *Cramer's V* = 0.30), cât și în mediul universitar ($\chi^2(16) = 1622.0$, $p < 0.01$, *Cramer's V* = 0.29). Printre motivele pentru care utilizatorii cred că este importantă sau foarte importantă introducerea studiului securității informatice se numără protejarea identității și a datelor personale, cunoașterea riscurilor la care sunt expuși utilizatorii tehnologiilor informatice sau evitarea fraudelor și a escrocheriilor.

Concluzii preliminare

Importanța rezultatelor aplicării acestui chestionar este dată de nevoia de înțelegere a nivelului culturii de securitate pe care populația din România o are în raport cu riscurile de securitate cibernetică și vulnerabilitățile din mediul online - offline.

În virtutea nevoii de a înțelege influențele instituțiilor supranaționale, materializate adesea prin deciziile, regulamentele, legislația internațională emise ori acțiuni politice, asupra populației din țările membre UE, cum este și România, sau a organizațiilor active în cadrul Uniunii Europene, trebuie să ne punem întrebări cu privire la

ce trebuie protejat sau exploatat, cum poate fi construită și dezvoltată legislația europeană într-un context de securitate incert și cum pot fi tratate vulnerabilitățile din sectorul cibernetic. Înțelegând că cea mai mare vulnerabilitate în acest domeniu este factorul uman, odată cu obținerea unor răspunsuri pertinente, putem trata subiectul guvernanței spațiului cibernetic din perspectiva securității naționale în dreptul celor două concepte, supranaționalism și realism. Totodată, suntem îndemnați să ținem cont de rolul statului în raport cu populația acestuia pentru asigurarea unui echilibru între decizia politică, progresul tehnologic, nevoile sociale, șamd. Statul român este național, suveran şi independent, unitar şi indivizibil. Ceea ce ne spune că România este pentru poporul român, *„un stat de drept, democratic şi social, în care demnitatea omului, drepturile şi libertățile cetățenilor, libera dezvoltare a personalității umane, dreptatea şi pluralismul politic reprezintă valori supreme"*[1]. Drept urmare, din perspectiva Constituției României, statul este direct responsabil de starea nației române. Starea și nivelul securității naționale sunt evaluate și în baza nivelului culturii de securitate și a gradului de conștientizare privind problematica de securitate a poporului român.

Având în vedere faptul că atât în România cât și în numeroase alte țări, în ceea ce privește analiza statistică, accentul este pus cu preponderență pe nivelul de semnificație statistică și mai puțin pe semnificația practică a efectelor, am optat pentru raportarea mărimii efectului în plus față de semnificația statistică (p) a diferențelor dintre frecvențele ce au fost identificate. Aceste mărimi ale efectului indică magnitudinea și importanța practică a rezultatelor și a concluziilor extrase din acest studiu.

Urmând modelul cercetării calitative[2], este important de menționat faptul că în cadrul fiecărui interviu a fost evaluat un număr de 27 întrebări principale în complexitatea cărora au fost atinse un număr

1. Constituția României, Titlul I, art.1, „*Statul Român*".
2. Jonathan Grix, *op. cit.* , pp.27-30.

de 57 aspecte punctuale (vezi Anexa nr.2) la care s-a răspuns prin aplicat chestionarul (vezi Anexa nr.1). Unele întrebări au fost evaluate cu DA/NU, evaluare scalară, evaluare prin bifarea unor căsuțe ce conțineau posibile răspunsuri general formulate și totodată, i s-a dat oportunitatea participantului ca în cadrul studiului să dezvolte răspunsul în câteva cuvinte. Chestionarele au fost aplicate în toate regiunile din România, fără a se ține cont de particularitățile societale din fiecare regiune. S-a dorit un studiu natural, neutru și echidistant față de nivelul social al persoanelor intervievate, motiv pentru care participanții nu au fost limitați sub nici o formă și au fost provocați să răspundă într-un mod sincer și direct.

Din analiza distribuției participanților la studiu pe categorii de competențe digitale, s-a constatat faptul că raportat la gradul ridicat de utilizare a echipamentelor și programelor informatice, un procent semnificativ de peste 50% au competențe medii de utilizare a acestor unelte, ceea ce este îmbucurător. Rezultatele menționate anterior sunt date în mod deosebit de procesul educațional din care elevii și studenții fac parte, dar și de cursurile din domeniul informatic urmate în scopul perfecționării continue sau reorientării profesionale ale angajaților, liber profesioniștilor ori a șomerilor. În medie posesorii de echipamente de comunicații moderne (*tablete, telefoane inteligente, laptop, diverse accesorii*) petrec utilizându-le un timp mediu între 3 și 10 ore/zi, subliniind faptul că jumătate dintre aceștia sunt activi în mediul online într-un procent cuprins între 50%-100%. Acest fenomen este dat de importanța acordată tehnologiei informației mai ales în mediul urban, unde un procent de peste 60% a recunoscut tehnologia digitală ca fiind destul de importantă, importantă și foarte importantă. Un motiv încurajator este dat de recunoașterea participanților la studiu - cu precădere de către elevi și studenți - a nevoii de securitate informatică în toate sectoarele societății, poziție argumentată și fundamentată de criminalitatea cibernetică, de experiențele din ultimii ani de progres tehnologic și de prognozele de insecuritate existente.

Considerații finale

Limitări și direcții viitoare de cercetare

În intervalul de timp 2015-2019, datorită spiritului critic manifestat pe de-o parte de comisia de îndrumare, iar pe de altă parte de practicienii în probleme de securitate cibernetică și cercetare a guvernanței securității mediului cibernetic, prezenta teză a fost modificată pentru a corespunde standardelor academice naționale privind forma și conținutul.

Astfel, dezbaterea rapoartelor de cercetare în cadrul întâlnirilor periodice, cât și comentariile primite în urma publicării parțiale a rezultatelor cercetării, au consolidat procesul de obținere a unor rezultatelor relevante întocmirii tezei și evidențierii faptului că guvernanța securității naționale este perfectibilă și performantă prin adoptarea unui management elitist al securității spațiului virtual, prin păstrarea unei balanțe de echilibru între conceptele reprezentative și specifice realismului și supranaționalismului.

Guvernarea domeniului cibernetic în contextul de securitate european este marcată de o evoluție strategică a reconstrucției europene. În concluzie, domeniul cibernetic poate fi guvernat de state

membre suverane într-o Uniune Europeană echilibrată între cele trei modele de guvernanță: *„guvernanță distribuită, guvernanță multilaterală și guvernanță de tipul multi-stakeholderismul"*.[1] Acest lucru nu exclude parteneriatele strategice ale țărilor membre sau ale Uniunii.

Datorită abordării metodelor de cercetare explorativă a securității domeniul cibernetic, sunt îndemnat să remarc faptul că buna guvernanță, percepută în contextul prezentei lucrări, este perfectibilă și încă departe de a fi un panaceu universal pentru dilema de securitate din spațiul cibernetic. În urma unei analize inductive a rezultatelor prezentei lucrări, identific realitatea necesității construcției unui forum pentru dezvoltarea unui nou model de bună guvernanță a arealului cibernetic prin asocierea cu această formă de guvernare a instituțiilor și organismelor guvernamentale, a sectorului privat și a actorilor societății civile. Sunt pe deplin încrezător că teza de față a deschis noi orizonturi de cercetare științifică a bunei guvernanțe în spațiul cibernetic. Odată cu motivația dată de identificarea acestor orizonturi, tangibile de altfel, precum și de atingerea în parte a obiectivelor propuse, doresc ca rezultatele obținute în prezenta teză să reprezinte bazele unor extinderi a cercetării de față și să aduc în atenția comunității academice noi perspective și rezultate ce privesc buna guvernanță a securității spațiului cibernetic.

Prin raportarea la celelalte patru arealuri strategice identificate, studiul bunei guvernanțe în spațiul cibernetic reprezintă în momentul de față domeniul cel mai lacunar unde am identificat, în ceea ce privește securitatea națională, o deosebită nevoie de control democratic din partea societății civile, obținut în asentimentul instituțiilor supranaționale sau naționale. Problematica escaladării spiralei de securitate reprezintă mai departe pentru mine un punct de interes

1. Andrew N. Liaropoulos, „Cyberspace Governance and State Sovereignty", în *Democracy and an Open-Economy World Order,* Edit. Springer International Publishing AG, 2017, p.29, https://www.researchgate.net/publication/316040640_Cyberspace_Governance_and_State_Sovereignty, accesat în data de 07.05.2019.

major, intenționând ca pe viitor să cercetez posibilități și ipoteze reale cu ajutorul cărora o nouă formă de bună guvernare a spațiului cibernetic să poată soluționa aspecte ale dilemei de securitate.

Finalmente, în ceea ce privește motivarea alegerii viitoarelor direcții de cercetare, un ultim argument este dat de abordarea strategică din ultimii zece ani pe care o nutresc asupra cercetării domeniului securității naționale în context cibernetic, prin capacitatea dinamică a celor trei elemente de a schimba direcția sau regulile în timpul *„jocului"*, anume: *progresul tehnologic, relațiile internaționale și securitatea.*

Precizări referitoare la contribuțiile personale

Pornind de la înțelegerea unei necesități de imparțialitate din partea cercetătorului privind subiectul cercetării, m-am detașat de orice influențe ce ar putea afecta cursul natural și obiectiv al lucrării. Fără a contesta faptul că oricând, subiectivitatea, chiar și într-o măsură neglijabilă, poate să apară, aceasta fiind datorată naturii noastre umane și apartenenței la un anumit grup sau clasă socială. Menționez că încă de la început analiza și abordarea problematicii s-a desfășurat la un grad ridicat de dificultate, finalmente concretizându-se, conform viziunii autorului, prin utilizarea unui mecanism propriu de analiză, sinteză și generare sistematică a rezultatelor, confirmându-le prin verificarea acestora în lumina studiului comparativ. Pentru o mai bună conceptualizare și înțelegere a cercetării, elementele de noutate sunt expuse la finele fiecărui capitol, reiterând în cele ce urmează printr-o concluzie comună, privind întregul studiu.

Până în prezent am identificat, în ceea ce privește subiectul tezei, o literatură de specialitate națională și internațională lacunară. Deși tendința este de a analiza într-un mod eclectic lucrarea de față, este important de menționat că o cercetare a relației dintre studiul guvernanței spațiului virtual în conceptul realismului ori a supranaționalis-

mului și managementul informațiilor vehiculate în mediul electronic raportat la cunoașterea nivelului culturii de securitate cibernetică în România, este un subiect care necesită o calitate multidisciplinară atât a autorului cât și a observatorului ori a criticului.

Datorită abordării sectorului guvernanței securității naționale în contextul studiul relațiilor internaționale, vorbim de o arie de cercetare de nișă, drept urmare doresc să evidențiez numărul relativ mic de membri ai comunității academice românești și internaționale care au în atenție studiul acestei teme sau cercetarea acestui domeniu în cadrul lucrărilor din spațiul public, fără a exista anumite restricții de clasificare.

Principalul element de noutate și originalitate adus domeniul de cercetare în care se înscrie teza de față este dat de obținerea unei relații de interdependență dintre cultura de securitate, nivelul de securitate națională existent și modalitatea de guvernanță a spațiului cibernetic.

Un element de noutate secundar este dat de construirea unui caz structurat pe demonstrarea argumentelor, solid susținut de nivelul culturii de securitate din România, raportat la managementul informațiilor vehiculate în mediul electronic pentru o bună guvernanță a spațiului cibernetic în context național și predominant european. Lipsa surselor bibliografice de specialitate orientate în direcția problematicii spiralelor de securitate cibernetică oferă o validare a demersul meu, realizat sub atenta monitorizare a profesorilor coordonatori. Validarea și confirmarea acestui demers de cercetare explorativă este dată și de obținerea de rezultate concrete în favoarea ipotezei potrivit căreia dilema de securitate cibernetică este o subdimensiune sau o terminologie hibridă, diferențiată de înțelesul uzual al dilemei de securitate prin transpunerea acesteia, conceptual, în contextul securității cibernetice.

În esență, prin asumarea rezultatelor cercetării dilemei de securitate cibernetică în perspectiva guvernanței spațiului virtual în conceptul realismului și supranaționalismului, înțeleg că, în urmă-

toarea decadă, până la apariția următoarei revoluții a tehnologiei în spațiul cibernetic, rolul organismelor publice și private, naționale și supranaționale, aste acela de a norma acest areal pentru diminuarea impactului adus de riscurile de securitate în toate mediile asupra cărora dilema de securitate își face simțită prezența. Deși este puțin probabilă o ofensivă militară de anvergură prin mediul cibernetic, apar din ce în ce mai des cazuri izolate cu un enorm impact financiar și de intimidare atât a personalităților juridice, cât și a persoanelor care folosesc acest mediu. Analizând din perspectiva studiilor relațiilor internaționale, diplomația a ajuns la un nou prag, acela de transformare și primește în portofoliu noi domenii de interes, diplomația cibernetică și diplomația digitală, care reprezintă în contextul globalizării interfața statelor, fiind și una dintre sursele generatoare de securitate principale.

Un considerent final este cel cu privire la viitoarea obligativitate de neproliferare a capabilităților cibernetice cu potențial ostil. Prin exemplele date și studiul efectelor acestora asupra statelor și alianțelor, se confirmă parțial posibilitatea identificată la nivel teoretic de utilizare a atacurilor cibernetice la nivel global în vederea producerii de efecte masiv dăunătoare din partea statelor. Cu toate acestea, sunt pe deplin încredințat că printr-o bună guvernanță și creștere a capacității de reziliență cibernetică a sistemelor informaționale la nivel global și totodată printr-o participare activă a statelor, uniunilor, formelor federative și alianțelor în vederea armonizării și reglementării consensuale a acestui domeniu, se poate păstra, indiferent de ideologia de guvernământ a statelor, un mediu cibernetic sigur și curat.

În cursul anilor de studiu, în ceea ce privește tema de cercetare aleasă, și datorită nevoii de a culege informația brută în forma ei primară și cât mai puțin prelucrată ori rafinată pentru crearea unei opinii originale și proprii, am participat și am prezidat o serie de conferințe, care au avut ca punct de interes și securitatea informației în mediile virtuale sub diferite forme. Fie că atenția a fost dusă către

aspectele societății cunoașterii, fie că au fost direcționate spre securizarea și protejarea datelor și a informației prin intermediul legislației ori a ramurilor sectorului tehnologic, scopul a fost unul singur, colectarea unui volum cât mai mare de informație vitală cercetării pentru procesul de sinteză și raportare a acesteia în conținutul acestei teze de doctorat. Cu siguranță, sacrificiile au meritat și consider că rezultatele sunt și vor fi de un real folos înțelegerii contextului de securitate cibernetic actual.

Concluzii

Conceptual, lucrarea de față poate fi considerată reflexia viziunii autorului asupra manierei proactive în care ar putea fi abordată interdependența dintre informație, guvernanța spațiului virtual, diplomația în spațiul cibernetic și securitatea cibernetică în contextul dezvoltării politicilor unitare europene. În acest sens, considerând că ipotezele de lucru au fost cercetate și rezultatele au fost credibil argumentate, lucrarea își propune să reitereze necesitatea alocării unui interes deosebit informației gestionate în mediile virtuale prin dezvoltarea și progresul științei securității și guvernanței spațiului cibernetic.

Deoarece transformarea oricărei problematici într-o dilemă devine un clișeu contemporan, autorul a construit întreaga lucrare bazându-se pe conceptul spiralei de securitate, unde fiecare capitol reprezintă un reper important în obținerea unei imagini clare asupra perspectivei de guvernanță a securității naționale prin managementul securității spațiului virtual între realism și supranaționalism. Demonstrând, prin intermediul celor șase capitole, problematica de securitate, putem afirma că tratarea dilemei de securitate a fost deschisă spre noi orizonturi de cercetare.

Ipotezele de cercetare prezentate la începutul prezentei lucrări au fost argumentate și de dinamica dilemei de securitate cibernetică, ale cărei efecte sunt materializate atât în plan cibernetic cât și în plan terestru / real. Aceasta, conform cercetărilor efectuate, prezintă particularități definitorii în raport cu celelalte medii strategice și operaționale. În procesul de argumentare și conceptualizare a ipotezelor lansate, s-a identificat un truism, spirala de securitate cibernetică este un subdomeniu bine definit al dilemei de securitate generale, efectele acțiunilor sau inacțiunilor din acest domeniu aducând efecte cinetice și reacții atât asupra elementelor terestre, cât și asupra deciziilor ale căror rezultate aduc la rândul lor rezultate mult amplificate - ale acțiunilor sau inacțiunilor din domeniul securității cibernetice (vezi *Anexa nr.3 Organigrama domeniilor guvernanței securității cibernetice*).

În urma procesului de colectare și analiză a materialelor necesare aprofundării studiului guvernanței securității naționale prin managementul securității spațiului virtual în contextul conceptelor realismului și supranaționalismului, s-a identificat o nouă perspectivă de analiză și cercetare a domeniului securității cibernetice. În viziunea autorului, identificarea contextului de securitate cibernetică actuală poate fi relevată prin evidențierea managementului informațiilor vehiculate în mediul electronic, studiul guvernanței spațiului virtual din prisma realismului și supranaționalismului, cercetarea aspectelor diplomației care acționează și în noul areal cibernetic, subliniind influențele aduse de politicile supranațional-europene în actuala stare geopolitică globală. Pentru a scoate în evidență motivația statelor și a formațiunilor supranaționale care își concentrează o anumită forță asupra statelor membre, autorul a adus în ecuație un studiu statistic privind cultura populației rezidente în România asupra securității cibernetice.

Analiza managementului riscului în organizațiile contemporane identifică în România o cultură de securitate cibernetică lacunară, de unde rezultă, în ultima decadă, multitudinea de breșe și incidente de

securitate apărute în toate sectoarele de interes, precum sunt serviciile, producția, industria șamd. Aceste evenimente, deloc de neglijat, produc un impact major asupra indivizilor și asupra organizațiilor în care aceștia activează. Prin identificarea nevoii acerbe de pregătire continuă pe specificul protecției informației și apărării împotriva factorilor de risc se confirmă rezultatele studiului de caz din ultimul capitol al tezei cu privire la gradul de cultură de securitate cibernetică a angajaților. În primul capitol s-a identificat faptul că, deși conceptele organizației, managementului riscului, managementului informației și condiția informației vitale într-o rămân aceleași ca până acum, apare o nevoie tot mai mare de aplicare a teoriei schimbărilor și desigur o readaptare a sistemului informațional la noile arealuri și provocări aduse de domeniul cibernetic și în unele cazuri o reconceptualizare a întregului sistem, după caz, în funcție de domeniul de activitate al fiecărei entități și gradul de implicare a instrumentelor domeniului cibernetic în activitatea propriu-zisă a organizației.

Cu toate că prezenta lucrare nu tratează problematica securității cibernetice strict în conceptul realismului sau a supranaționalismului, apare într-un mod natural nevoia de a răspunde la provocările ridicate de relația dintre cele două concepte în raport cu securitatea cibernetică. Odată cu analiza celor două concepte, se obține o poziție a României în calitate de *„stat național, suveran şi independent, unitar şi indivizibil”*[1] și în același timp ca stat membru al UE.

Unul dintre cele mai importante aspecte care au captat atenția autorului a fost dimensiunea domeniului cibernetic, care reprezintă o noțiune limitativă a granițelor terestre reglementate de state.[2] Drept urmare, indiferent în lumina cărui concept este analizat actul de guvernanță a spațiului virtual, trebuie înțeles și abordat respectând echilibrul de forțe și suveranitate a statelor și a formelor de organizare supranaționale. Abordarea se dovedește a fi mai degrabă una

1. Constituția României, Titlul I, art.1, *„Statul Român”*.
2. *Ibidem*, Titlul I, art.3, *„Teritoriul”*.

explorativă decât una exhaustivă, având ca scop primar plasarea domeniului securității cibernetice pe o hartă a relațiilor internaționale raportată la concepte - cel puțin teoretice - de guvernanță a statelor sau a alianțelor în context geopolitic actual.

Noutatea aceasta apare ca urmare a abordării unui spațiu care nu este reglementat și normat suficient, precum este spațiul terestru de exemplu. Abordarea nu poate fi decât una explorativă, deoarece încă sunt multe domenii de cercetare care își abandonează resursele fizice limitate și migrează spre acest nou areal virtual numit spațiu cibernetic, ale cărui limite sunt date de nevoile noastre de dezvoltare.

Odată înțeleasă poziția României ca stat suveran[1], membru al unei alianțe supranaționale în actualul context de securitate global, este inevitabilă atingerea și tratarea subiectului îndeplinirii actului diplomatic cu sprijinul resurselor puse la dispoziție de progresul tehnologic în vastul areal cibernetic. În capitolul alocat tratării problematicii diplomației în spațiul cibernetic s-au lămurit aspecte referitoare la greșita interpretare a conceptelor precum *„diplomația cibernetică"* / *„diplomația digitală"* și argumentarea necesității dezvoltării acestora pentru obținerea de rezultate diplomatice superioare celor obținute în absența acestor concepte.

Unul dintre pilonii esențiali ai guvernanței securității naționale este desigur legislația aplicabilă specifică, reliefată de influențele politice europene privind securitatea informației electronice în actuala stare geopolitică globală. În context legislativ, *„principiul supremației dreptului Uniunii Europene (UE) asupra dreptului național al statelor membre este unul dintre principiile fundamentale, care alături de principiul efectului direct şi aplicabilitatea imediată, definesc Uniunea Europeană ca entitate sui generis a dreptului internațional.[…] În lumina jurisprudenței Curții de Justiție invocată în prezentul material, în raport cu poziția Curților Constituționale naționale, putem afirma că, în practică, asistăm la un compromis între competențele judecătorului UE şi cele ale judecătorului*

1. Ibidem, Titlul I, art.2, *„Suveranitatea"*.

național. Astfel, jurisprudența Curții de Justiție va avea întotdeauna întâietate şi se va bucura de o prezumție de interpretare autentică a dreptului UE. Curțile Constituționale, pe de altă parte, vor păstra o competență reziduală, care nu va putea fi activată decât în cazuri excepționale în care ar fi puse în pericol principiile fundamentale ale ordinii constituționale naționale sau atribuirea de competențe între Uniunea Europeană şi statele sale membre."[1] Urmare a acestui principiu, s-a analizat abordarea de politică externă a României și s-a considerat oportună identificarea problematicii securității cibernetice din perspectiva organismelor internaționale şi implicarea României în soluționarea acesteia.

Din analiza modelelor internaționale și organismelor europene, respectiv organismelor naționale cu atribuții în domeniul securității cibernetice, s-a ajuns la observarea strategiilor de securitate cibernetică în zona UE și în raport cu restul lumii și la propunerea de a identifica nevoi și oportunități de implicare pro activă, pe termen mediu și lung, din partea întregului front comun al UE în acest domeniu.

Ultimul capitol al prezentei teze este pe de-o parte o confirmare a rezultatelor obținute pe parcursul cercetării, iar pe de altă parte un element de noutate în ceea ce privește nivelul de cultură de securitate cibernetică a populației rezidente în România și gradul de conștientizare a populației în raport cu vulnerabilitățile și riscurile existente în arealul cibernetic, precum și în relația acțiuni în mediul virtual - impact în arealul terestru. Raportul statistic obținut în urma studiului de caz expus în ultimul capitol poate fi considerat o veritabilă resursă în abordarea viitoarelor direcții de cercetare privind guvernarea securității cibernetice.

Strategia de cercetare a avut ca obiectiv o identificare foarte specifică a celor mai importante aspecte privind securitatea persoanelor

1. Răzvan Horaţiu Radu, Conferinţa Internaţională: *Rolul justiției constituționale în protecţia valorilor statului de drept, Manifestare dedicată celei de-a 20-a aniversări a Constituției Republicii Moldova*, „Prioritatea ordinii juridice UE asupra dreptului național", Chișinău, 8-9 septembrie 2014, http://www.constcourt.md/public/files/file/conferinta_20ani/programul_conferintei/Razvan_Horatiu_Radu.pdf, accesat în data de 11.03.2019.

în arealul cibernetic. S-au cules date, conceput chestionare, validat chestionare, aplicat chestionare, centralizat date și în cele din urmă s-au analizat aceste date atât din punct de vedere cantitativ cât și calitativ.

În această ordine de idei, se poate concluziona că buna guvernanță a securității cibernetice înseamnă în mod direct securizare rațională în folosul tuturor aspectelor vieții persoanei care preia în context cibernetic denumirea de utilizatorilor. Fără a subclasa importanța prosperității economice și securitatea națională, se poate confirma că buna guvernanță face o directă referire și la modul de asigurare a integrității și prosperității acestor două elemente în spectrul cibernetic de activitate și influență. Sinergia între actorii statali și nestatali relevanți, în contextul unei bune guvernări pentru dezvoltarea durabilă a spațiului cibernetic, este una crucială, atât pentru a proteja suveranitatea națională, cât și pentru a consolida alianțele supranaționale, cu un scop comun, progresul. În mod specific, în ceea ce privește guvernanța securității cibernetice a României, se poate concluziona că este necesară o expunere cât mai exhaustivă a punctelor centrale și definitorii și o mai multă determinare în ceea ce privește gestionarea resurselor și utilizarea prezentelor sau viitoarelor oportunități strategice în vederea obținerii cel puțin a unor avantaje prognozate din raportul relațiilor internaționale ale României în context european și desigur global.

Firul central al viziunii autorului este dat de identificarea unei noi perspective asupra managementului securității spațiului cibernetic. Elementele de bază ale acestei noi perspective sunt evidențiate atât prin cuvintele cheie de la începutul lucrării, cât și definitoriu în conținutul capitolelor prezentei teze. Desigur, în viziunea autorului, această perspectivă reprezintă un cadru de analiză nou și un element de noutate care poate aduce lumină asupra viitoarelor direcții de cercetare în domeniul științelor relațiilor internaționale și studiilor de securitate.

De asemenea, în contextul prezentei lucrări, datorită caracterului multidisciplinar al acesteia, această nouă perspectivă de analiză mai sus menționată consider că își poate aduce aportul în identificarea unor noi provocări în domeniul cercetării și studiilor diplomatice și a celor din aria științelor comunicațiilor și tehnologiei informației.

Tratarea temei alese a fost inițial studiată și ulterior cercetată cu scopul de a aduce o completare din punct de vedere științific a cunoștințelor comunității academice și de a încerca să transpună problematica prin prisma conceptelor realismului și a supranaționalismului. Validarea studiului este desigur lăsată la latitudinea criticilor și în speranța unor reacții constructive, dorința autorului este de a dezvolta în parte sau în întregime subiectul de cercetare ales.

Bibliografie

Cărți (inclusiv ediții electronice)

***Academia Română, Institutul de lingvistică „Iorgu Iordan", *Mic dicționar academic*, Ediția a II-a, Edit. Univers Enciclopedic, București, 2010.

***Academia Română, Institutul de Lingvistică „Iorgu Iordan", *Dicționarul explicativ al limbii române* (ediția a II-a revizuită și adăugită), Editura Univers Enciclopedic, București, 1998.

***Academia Română, Institutul de Lingvistică „Iorgu Iordan", *Dicționarul explicativ al limbii române*, Editura Univers Enciclopedic Gold, București, 2012.

ABLON, Lillian, BINNENDIJK HODGSON, Anika, , QUENTIN E., BILYANA, Lilly, ROMANOSKY, Sasha, SENTY, David, THOMPSON, Julia A., *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*, Edit. RAND Corporation, Santa Monica, USA, 2019.

ALECU, Gheorghe, BARBĂNEAGRĂ, Al., *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic*, Edit. Pinguin Book, București, 2006.

ALEXANDRU, Ioan, *Structuri Mecanisme și Instituții Administrative*, vol.2, Edit. Sylvi, București, 1996,

BĂCANU, Bogdan, *Organizație publică - Teorie și management*, Edit. Polirom, Iași, 2008.

BÎZOI, Mihai, *Sisteme Suport pentru Decizii Bazate pe Comunicații* (teză de doctorat), Academia Română, Institutul de Cercetări pentru Inteligență Artificială, București, 2010.

BLAIKIE, Norman, *Modele ale cercetării sociale: Producerea cunoașterii*, Ediția a II-a,, Edit. CA Publishing, Cluj-Napoca, 2010.

BRANDON, Valeriano, MANESS, Ryan C., *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Edit. Oxford University Press, New York, 2015.

BRUCE, Russett, ONEAL, John, *Triangulating Peace, Democracy, Interdependence, and International Organizations*, Edit. W.W. Norton & Company, New York-Londra, 2001.

BUZAN, Barry, *Popoarele, statele şi teama. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Edit. Cartier, Chișinău, 2000.

BUZAN, Barry, WÆVER, Ole, DE WILDE, Jaap, *Securitatea. Un nou cadru de analiză*, Edit. CA Publishing, Cluj-Napoca, 2011.

CĂMĂRĂȘAN, Adrian V., *Informații clasificate - Note de curs*, Edit. CA Publishing, Cluj-Napoca, 2014.

CERI, Stefano, BOZZON, Alessandro, BRAMBILLA, Marco, DELLA VALLE, Emanuele, FRATERNALI, Piero, QUARTERONI, Silvia, *Web Information Retrieval*, Edit. Springer, Berlin, 2013.

CHIRLESAN, Georgeta, *Strategia de securitate naţională a României: evoluții şi tendințe între securitatea regională şi cea euro-atlantică*, Editura Academiei Forțelor Terestre „Nicolae Bălcescu”, Sibiu, 2013.

CHRISTOU, George, *Cybersecurity in the European Union - Resilience and Adaptability in Governance Policy*, Edit. Palgrave Macmillan, 2016.

CRAIG, Anthony J.S., Valeriano, Brandon, *Realism and Cyber Conflict: Security in the Digital Age*, Edit. E-International Relations Publishing, Bristol, Anglia, 2018.

CRAMÉR, Harald, *Mathematical Methods of Statistics*, Edit. Princeton University Press, Princeton, 1946.

DUICĂ, Anișoara, *Management*, Ediția a II-a (revizuită și adăugită), Edit. Bibliotheca, Târgoviște, 2008.

FILIP, Florin Gheorghe, *Sisteme suport pentru decizii*, Edit. Tehnica, București, 2007.

FLASIŃSKI, Mariusz, *Introduction to Artificial Intelligence*, Edit. Springer, Elveția, 2016.

FREYBERG-INAN, Annette, *What Moves Man: The Realist Theory of International Relations and Its Judgement of Human Nature*, State University of New York Press, Albany, SUA, 2004.

FRIEDMAN, Thomas L., *The Lexus and the Olive Tree - Understanding Globalization*, Edit. Farrar, Straus and Giroux, New York, 2000.

GRIFFITHS, Martin, *Relații internaționale. Școli, curente, gânditori*, Editura Ziua, București, 2003.

GRIX, Jonathan, *Demistificarea cercetării postuniversitare: De la masterat la doctorat*, Edit. CA Publishing, Cluj-Napoca, 2014.

HOBEANU, Tudor, HOBEANU, Loredana, *Management - Fundamentele managementului organizației*, Edit. Sitech, Craiova, 2007.

ILIE, Gheorghe, CIOBANU, Ion, NOUR, Aurel, *Confruntarea informațională și protecția informațiilor*, Edit. Detectiv, București, 2006.

ILIE, Gheorghe, *De la management la guvernare prin risc*, Edit. Detectiv/Edit. UTI Press, București, 2009.

ILIE, Gheorghe, *Riscul-Măsura Incertitudinii - Elemente conceptuale, corelații și determinări*, Edit. UTI Press, București, 2011.

IVAN, Adrian-Liviu, *Statele Unite ale Europei: Uniunea Europeană între interguvernamentalism şi supranaționalism*, Editura Institutul European, Iași, 2007.

JAIN, N.K., *Organisational Behavior*, Edit. Atlantic, New Delhi, 2005.

KALDOR, Mary, *Securitatea Umană*, Ed. CA Publishing, Cluj-Napoca, 2010.

KEEN, Peter G.W., *Every Manager's Guide to Information Technology*, Edit. Harvard Business School Press, 1995.

KURKI, Milja, SMITH, Steve, *Internationale Relations Theories. Discipline and Diversity*, Edit. Oxford University Press, Oxford, 2006.

KYDD, Andrew H., *Trust and mistrust in international relations*, Edit. Princeton University Press, Princeton, New Jersey, SUA, 2005.

LANGNER, Ralph, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, Edit. The Langner Group, Arlington, Hamburg, 2013.

LIPSCHUTZ, Ronnie D., *On Security*, Edit. Columbia University Press, New York, 1995.

LOMAX, Richard G., HAHS-VAUGHN, Debbie L., *Statistical concepts: A second course* - Ediția a 4-a, Edit. Routledge, New York, 2012.

LORD, Kristin M., SHARP, Travis, *America's Cyber Future, Security and Prosperity in the Information Age*, Edit. Center for a New American Security, Washington, DC, 2011.

MEYERS, Diana T., *Political Realism And International Morality: Ethics In The Nuclear Age* , Edit. Routledge Taylor & Francis Group, New York, SUA, 2019.

MORGENTHAU, Hans J., *Politics among Nations: The Struggle for Power and Peace*, New York, Edit. Alfred A. Knopf, 1949.

MROZ, John Edwin, *Beyond Security, Private Perceptions Between Arabs and Isrealis*, Ed. International Peace Academy, New York, 1991.

NIȚU, Ciprian, *Cosmopolitismul-Către o nouă paradigmă în teoria politică*, Edit. Adenium, Iași, 2014.

NIȚU, Ionel, *Analiza de Intelligence, O abordare din perspectiva teoriilor schimbării*, Edit. Rao, București, 2012.

NYE, Joseph S., *The Future of Power*, Edit. Public Affairs, New York, 2011.

OPREA, Dumitru, *Protecția și securitatea informațiilor*, ediția a II-a, Edit. Polirom, Iași, 2007.

POPA, Iulian, *Securitatea și guvernanța spațiului cibernetic contemporan (teză de doctorat)*, Universitatea Babeș-Bolyai, Cluj-Napoca, 2015.

RADU, Ioan, *Informatică și management - O cale spre performanță*, Edit. Editura Universitară, București, 2005.

RĂDOI, Mireille, *Serviciile de informații și decizia politică*, Edit. Tritonic, București, 2003.

RICHARD, Clarke A., KNAKE, Robert K., *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Ecco, SUA, 2010.

RIORDAN, Shaun, *The Strategic Use of Digital and Public Diplomacy in Pursuit of National Objectives*, Edit. Top Open Printing Sytems S.L., Barcelona, 2016.

ROBINSON, Paul, *Dicționar de securitate internațională*, Edit. CA Publishing, Cluj-Napoca, 2010.

ROBSON, Colin, *Real World Research: A resource for Social Scientists and Practitioner-Researchers*, Ediția a-II-a, Edit. Blackwell Publisher, Oxford, 2002.

SARCINSCHI, Alexandra, *Elemente noi în studiul securității naționale şi internaționale*, Editura Universității Naționale de Apărare, București, 2005.

SENESE, Paul D., VASQUEZ, John A., *The Steps to War: An Empirical Study*, Princeton University Press, Princeton, 2008.

SPENCE, Jymmy W., „A case study analysis of organizational communication effectiveness between user-managers and information service department personnel” (lucrare de diserta-

ție-Administrarea afacerilor), Texas Tech University, Texas, 1978.

STEFANO, Guzzini, *Realism şi Relații Internaționale - Povestea fără sfârșit a unei morți anunțate: realismul în relațiile internaționale și în economia politică internațională*, Edit. Institutul European, Iași, 2000.

STOLL, Clifford Paul, *The Cukoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, New York, Doubleday, 1989.

TAKEUCHI, Nonaka, H., *The knowledge-creating company - How Japanese companies create the dynamics for innovation*, Edit. Oxford University Press, New York, 1995.

TALEB, Nassim Nicholas, *Lebăda neagră - Impactul foarte puțin probabilului*, Edit. Curtea Veche, București, 2008.

THOMAS, Rid, *Cyber War Will Not Take Place*, Edit. C Hurst & Co Publishers Ltd., Londra, 2013.

TZU, Sun, *Arta Războilui*, Ed. Imprimeria CORESI, București.

ȚICU, Dorina, *Politicile publice. Raționalitate și decizie în spațiul administrativ*, Edit. Adenium, Iași, 2014.

VASIU, Ioana, VASIU, Lucian, *Criminalitatea în cyberspațiu*, Edit. Univers Juridic, București, 2011.

VASIU, Ioana, Vasiu, Lucian, *Informatică Juridică și Drept Informatic*, Editura Albastră, Cluj-Napoca, 2009.

VASQUEZ, A. John, *The War Puzzle*, Cambridge University Press, Cambridge , 1993.

VLĂDOIU, Nasty, *Protecţia Informațiilor. De la concept la implementare*, Edit. Tritonic, București, 2005.

VLĂSCEANU, Mihaela, *Organizatii și comportament organizational*, Edit. Polirom, Iași, 2003.

VLĂSCEANU, Mihaela, *Organizația: proiectare și schimbare - Introducere în comportamentul organizațional*, Edit. Comunicare, București, 2005.

VON GEUSAU, Frans Alphons Maria Alting, PELKMANS, Jacques, *National Economic Security: Perceptions, Threats, and Policies*, Edit. John F. Kennedy Institute, Olanda, 1982.

WALTZ, Kenneth N., *Theory of* International Politics, Edit. Addison-Wesley Publishing Company, Londra,1979.

WOLFERS, Arnold, Discord and Collaboration: Essay on International Politics, Edit. The Johns Hopkins Press, Baltimore, Maryland, SUA, 1962.

WRIGHT-NEVILLE, David, Dicționar de Terorism, Edit. CA Publishing, Cluj-Napoca, 2010.

YIN, Robert K., Case Study Research: Desi*gn and Method, Ediția a-V-a*, Edit. SAGE Publications, Thousand Oaks, 2014.

Articole științifice și capitole în cărți (inclusiv ediții electronice)

ABWNAWAR, Nasser, „A Policy-Based Management Approach to Security in Cloud Systems", Working Paper, De Montfort University Leicester, 2020.

ACHARYA, Avidit, RAMSAY , Kristopher W., "The Calculus of the Security Dilemma", în *Quarterly Journal of Political Science* Vol. 8, nr. 2, Princeton, USA, 2013.

ARQUILLA, John, RONFELDT, David, „Cyberwar is Coming!", în *Comparative Strategy*, Vol.12, Nr. 2, 1993.

BARNA, Cristian, „Pregătire și formare în societatea cunoașterii", în *Intelligence*, Nr. 35, București, 2017.

BASHARI RAD, Babak, AKBARZADEH, Nafisseh, ATAEI, Pouya, KHAKBIZ ,Yasaman, „Security and Privacy Challenges in Big Data Era", în *International Journal of Control Theory and Applications*, Vol. 9, nr.43, 2016.

BHARADWAJ, Anandhi, EL SAWY, Omar A., PAVLOU, Paul A., Venkatraman, N., „Digital Business Strategy: Toward a Next Generation Of Insights", în *MIS Quarterly*, Vol. 37 Nr. 2, Ed. MISRC, Minnesota, SUA, 2013.

BJOLA, Corneliu, „Digital diplomacy - the state of the art", în *Global Affairs*, Vol.2, Nr. 3, Edit. Routledge Taylor & Francis Group, 2016.

BJÖRCK, Fredrik, HENKEL, Martin, STIRNA, Janis, ZDRAVKOVIC, Jelena, „Cyber Resilience - Fundamentals for a Definition", în *New Contributions in Information Systems and Technologies, Advances in Intelligent Systems and Computing*, Vol.353, Edit. Springer, Cham, 2015.

BODEAU, Deborah J., GRAUBART, Richard, „Cyber Resiliency Engineering Framework", în *MITRE Tehnical Report (2011)*, Bedford, Massachusetts, 2011.

BOGZEANU, Cristina, „Echilibrul de putere şi mediul de securitate", în *Implicații ale teoriilor echilibrului de putere şi a echilibrului de interese într-un sistem internațional multipolar (conference proceedings)*, Edit. Universității Naționale de Apărare „Carol I", Bucureștii, 2011.

BOTTOU, Léon, CURTIS, Frank E., NOCEDAL, Jorge, „Optimization Methods for Large-Scale Machine Learning", în *SIAM Review*, Vol. 60, Nr. 2, 2018.

CLAIN, Alexandru Nicolae, „Consiliul Europei - instituție supranațională sau conferință interguvernamentală?", în *Continuitate și schimbare în guvernanța europeană*, Vol. 4, Nr. 1, 2010.

COHEN, Jacob, „A power primer", în *Psychological Bulletin, Quantitative Methods in Psychology*, nr.112, Edit. American Psychological Association, Washington (DC), 1992.

CONKLIN, William Arthur, SHOEMAKER, Dan, „Cyber-Resilience: Seven Steps for Institutional Survival", în *The EDP Audit,*

Control, and Security Newsletter, Vol.55, Nr. 2, Edit. Taylor & Francis Group, 2017.

CRAIG, Anthony, VALERIANO, Brandon, „Conceptualising cyber arms races", în *Proceedings of the 8th International Conference on Cyber Conflict (CyCon)*, Edit. NATO CCD COE Publication, Tallin, 2016.

DAASE, Cristopher, „The English School", în *Theories of International Relations*, Edit. Routledge Taylor & Francis Group, Londra, 2014.

DAVIDESCU, Roxana, TRIFU, Alexandru, „O perspectivă mentală de valoare în teoria deciziei în condiții de risc", în *Theoretical and Applied Economics, nr. 7 (502)*, Edit. Asociația Generală a Economiștilor din România - AGER, București, 2006.

DUNN CAVELTY, Myriam, „Cybersecurity in Switzerland", în *Springer Briefs in Cybersecurity*, Edit. Springer International Publishing, Zürich, 2014.

DUNN, Cavelty Myriam, „Cyber-Security and Threat Politics: US efforts to secure the information age", în *CSS Studies in Security and International Relations*, Prima Ediție, Edit. Routledge, London, UK, 2008.

ERIK, Gartzke, „The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth", în *International Security* Vol.38, Nr. 2, 2013.

ERIKSSON, Johan, GIAMPIERO, Giacomello, „The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", în *International Political Science Review,* Vol. 27, nr. 3, 2006.

FRUNZETI, Teodor, BĂRBULESCU, Cristian, „Cultura de securitate și reziliența națională la amenințările hibride, Reziliența național la amenințările hibride și cultura de securitate. Un cadru de analiză.", 2018.

GHENGHEA, Georgeta, STRATAN, Zinaida, ZAVTUR, Natalia, „Impactul culturii informației asupra utilizatorilor doctoranzi (studiu de caz)", 2019, http://repository.utm.md/handle/5014/1667, accesat în data de 23.07.2019.

GIBLER M. Douglas, RIDER J. Toby, HUTCHISON L. Marc, „Taking Arms Against a Sea of Troubles: Conventional Arms Races During Periods of Rivalry", în *Journal of Peace Research*, Vol. 42, Nr. 2, Edit. Sage Publications, Ltd., Londra, 2005.

GLASER Charles L., "When Are Arms Races Dangerous? Rational versus Suboptimal Arming", în *International Security*, Vol.28, Nr. 4, 2004.

GLASER, Charles L., „Realists as Optimists: Cooperation as Self-Help", în *The Perils of Anarchy: Contemporary Realism and International Security*, The MIT Press, Massachusetts, 1995.

GLASER, Charles L., KAUFMANN, Chaim, „What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics)", în *International Security*, Vol. 22, nr. 4, Massachusetts,1998.

GOLDMAN, Emily, ARQUILLA, John O., „Defense Analysis", în *Cyber Analogies*, Edit. Naval Postgraduate School, Monterey, California, 2014.

GORTZAK Yoav, HAFTEL Z. Yoram, SWEENEY, Kevin, "Offense-Defense Theory: An Empirical Assessment", în *Journal of Conflict Resolution*, Vol. 49, Nr. 1, Edit. Sage Publications, Inc., Ohio, SUA, 2005.

IANCU, Dumitru, „Informația Sursă de avantaj concurențial", în *Anuarul Academiei Forțelor Terestre "Nicolae Bălcescu"*, 2007.

ILAN Manor, ELAD Segev, KAMPF, Ronit, „Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter", în *The Hague Journal of Diplomacy*, Vol.10, nr.4, Haga, 2015.

IVAN, Adrian Liviu, „Constructivismul și Integrarea Europeană: Contribuții și Limite" în *Hello World!: Contemporaneitate și provocările globalizării*, Edit. CA Publishing, Cluj-Napoca, 2014.

IVAN, Adrian-Liviu, „Governance and "European Constitution", în *Transylvanian Review of Administrative Sciences*, Vol.4, nr.22, 2008.

JOYCE, A. L., PETIT, F. D., PHILLIPS, J. A., NOWAK, L. B., EVANS, N. J., „Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program", în *Raport Tehnic* OSTI.gov, Global Security Sciences Division, Argonne National Laboratory, 2017.

KANNIAINEN, Vesa, „Cyber Technology and the Arms Race", în *HECER Discussion Paper No. 424*, Helsinki, 2018.

KEIR, Lieber, „The Offense-Defense Balance and Cyber Warfare", în *Cyber Analogies*, Institutional Archive of the Naval Postgraduate School, Monterey, 2014.

KLIMBURG, Alexander, ZYLBERBERG, Hugo, „Cyber Security Capacity Building: Developing Access", în *NUPI Report nr.6*, Edit. Norwegian Institute of International Affairs, Oslo, 2015.

KOVAČEVIĆ, Aleksandar, IVANOVIĆ, Dragan, MILOSAVLJEVIĆ, Branko, Konjović, ZORA, Dušan Surla, „Program electronic library and information systems", în *Automatic extraction of metadata from scientific publications for CRIS systems*, Vol. 45, Nr. 4.

LAYNE, Christopher, „The Unipolar Illusion: Why New Great Powers Will Rise", în *International Security*, Vol. 17, Nr. 4, Massachuset, Edit. MIT Press, Massachuset, 1993.

LIAROPOULOS, Andrew N., „Cyberspace Governance and State Sovereignty", în *Democracy and an Open-Economy World Order,* Edit. Springer International Publishing AG, 2017.

LINDSAY, Jon R., „Stuxnet and the Limits of Cyber Warfare", în *Security Studies*, Vol. 22, Nr. 3, Taylor&Fracis Online.

LORD, M. Kristin, Sharp Travis, „America's Cyber Future: Security and Prosperity in the Information Age", în *Center for a New American Security,* Vol.1, Center for a New American Security, 2011.

LUBELL, Mark, „Governing Institutional Complexity: The Ecology of Games Framework", în *The Policy Studies Journal,* Vol. 41, Nr. 3, 2013.

MANOR, Ilan, SEGEV, Elad, KAMPF, Ronit, „Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter", în *The Hague Journal of Diplomacy*, Vol.10, nr.4, Haga, 2015.

MEARSHEIMER, John Joseph, "Structural Realism", în *International Relations Theories:Discipline and Diversity,* Oxford University Press, Oxford, 2006.

MILLER, John P., „Atomism, Pragmatism, Holism", în *Journal of Curriculum and Supervision*, Vol.1, nr.3, 1986.

MITU, Theodor, MITU, Daniela, „OSINT - la granița dintre secret și public", în *Revista Română de Studii de Intelligence*, nr. 4, Edit. Serviciul Român de Informații, București, 2010.

MURRAY, Lori, BUDENSKE, John, GANGOPADHYAY, Shubhagat, FINSTAD, Robert K., „Cyber resilience and integrity self-awareness of mobile autonomous systems", în *Proceedings of the SPIE Defense + Security*, 2018.

MUSCU, Georgiana Roxana, „Lipsa exercitării suveranității ca un risc de vulnerabilitate pentru securitatea internațională (Cazul Ucrainei)", în *Conferința Științifică Internațională Strategii XXI - complexitatea şi dinamismul mediului de securitate*, Vol.1, Edit. Universității Naționale de Apărare „Carol I", București, 2015.

NEUFEIND, Max, O`REILLY Jacqueline, Ranft Florian, *Work in the digital age: Challenges of the fourth industrial revolution*, Edit. Rowman&Littlefield International, Londra, 2018.

NIȚĂ, Cristian, „Securitatea Naţională - O Perspectivă Academică”, http://www.nos.iem.ro/bitstream/handle/123456789/33/4.1.Sec%20Academic%20nita.pdf?sequence=1&isAllowed=y, accesat în data de 30.07.2019.

NYE, Joseph S., „Soft Power”, în *Foreign Policy*, no.80, Edit. Washington Post, Washington, 1990.

OTTIS, Rain, „Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective”, Tallinn, Estonia, 2019.

PERU-BALAN, Aurelia, BAHNEANU, Vitalina, „Războiul informațional, Propaganda, Fake-News: Controlul asupra percepției publice”, în *Moldoscopie*, nr.1, Vol. LXXX, Chișinău, 2018.

POPA, Iulian F., „Metoda scenariilor în analiza informațiilor de securitate națională. Studiu teoretic-aplicativ”, în *Globalizare. Identitate. Securitate*, Editura CA Publishing, Cluj-Napoca, 2015.

POWELL, Robert, „Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate”, în *International Organization*, Vol. 48, Nr. 2, The MIT Press, Massachusetts, 1994.

REARDON, Robert, CHOUCRI, Nazli, “*The Role of Cyberspace in International Relations: A View of the Literature*”. Lucrare prezentată în 2012 la Convenția Anuală ISA, San Diego, 2012.

ROBERT, Jervis, “Cooperation Under the Security Dilemma”, în *World Politics*, Vol.30, Nr. 2,, Edit. The Johns Hopkins University Press, 1978.

ROG, Anton, CONDRUȚ, Cristian, „Evoluția amenințării cibernetice”, în *Intelligence în serviciul tău*, nr.38, Edit. SRI, București, 2019.

SAMEK, Wojciech, MŰLLER, Klaus-Robert, „Towards Explainable Artificial Intelligence”, în *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, Edit. Springer, 2019.

SCHMIDT, Andreas, „The Estonian Cyberattacks", în *The fierce domain –conflicts in cyberspace 1986-2012* (ed. Jason Healy), Edit. Atlantic Council, Washington, D.C, 2013.

SINHA, Aseema, „Building a Theory of Change in International Relations: Pathways of Disruptive and Incremental Change in World Politics", în *International Studies Review*, Vol. 20, Nr. 2, Oxford University Press, Oxford, 2018.

SISTROM, Christopher L., GARVAN, Cynthia W., „Proportions, odds, and risks", în *Statistical Concepts Series, Radiology*, Vol.230, Edit. University of Florida College of Medicine, Gainesville, 2004.

STRATAN, Alexandra, „Proliferarea noilor tehnologii. Inteligența artificială pe câmpul de luptă", în *Revista Intelligence Online*, 2019.

SUSAN, Sample G., „Arms Races and Dispute Escalation: Resolving the Debate", în *Journal of Peace Research*, Vol. 34, Nr. 1, Edit. Sage Publications, 1997.

ȘINCA, George-Marius, „Cibercriminologia - O analiză succintă a fenomenului de tranziție de la criminalitatea tradițională la cibercriminalitate", în *AGORA International Journal of Juridical Sciences*, Nr. 1, Oradea, 2015.

ȘINCA, George-Marius, „Managementul Elitelor în Managementul Riscurilor Cibernetice", în *De la Elitele Securității la Securitatea Elitelor*, Edit. Presa Universitară Clujeană, Cluj-Napoca, 2017.

TALIAFERRO, J.W., „Security Seeking under Anarchy: Defensive Realism Revisited", în *International Security*, Vol. 25, Nr. 3, Massachusetts, 2000.

TALIAFERRO, Jeffrey W., „Security Seeking under Anarchy: Defensive Realism Revisited", în *International Security*, Vol.25, nr.3, The MIT Press Journals, Massachusetts, 2000.

THURAISINGHAM, Bhavani M., KHAN, Latifur, MASUD, Mehedy, HAMLEN, Kevin W., „Data Mining for Security Applicati-

ons", în *Proceedings 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, 2008

TIRZIU, Andreea-Maria, „Protection and security of information at the level of national public authorities from Romania", în *MPRA Munich Personal RePEc Archive*, Munchen, 2015.

TODOR, Cătălina, „The topicality of security dilemma's spiral model in analysing the international environment", în *Strategic Impact*, Vol.63, Nr. 2, București, 2017.

TUFĂ, Laura, „Diviziunea digitală. Accesul şi utilizarea internetului în România, comparativ cu țările Uniunii Europene", în *Calitatea Vieţii-Revistă de politici sociale*, anul XXI, nr. 1-2, Editura Academiei Române, București, 2010.

UNGUREANU, Radu-Sebastian, CUCUTĂ, Radu-Alexandru, „Europenization as a hegemonic project: EU influence in approaching the security issues in the Balkans", în *New Challenges to the Balkan Security - Thematic Collective Book*, Vol.3, Edit. Ivis, Veliko Târnovo, Bulgaria, 2016,.

VALERIANO, Brandon, „The Tragedy of Offensive Realism: Testing Aggressive Power Politics Models", în *International Interactions,* Vol. 35, Nr. 2, Londra, 2009.

VAN EVERA, Stephen, "Offense, Defense, and the Causes of War", în *International Security*, Vol.22, Nr. 4, Edit. Cornell University Press, New York, 1998.

VAN EVERA, Stephen, „Defense, and the Causes of War", în *International Security, Offense*, Vol.22, 1998.

VAN PUYVELDE, Damien, COULTHART, Stephen, HOSSAIN, Shahriar M., „Beyond the buzzword: big data and national security decision-making", în *International Affairs,* Vol. 93, Nr. 6, 2017.

VASILE, Cătălin George, „Inteligența artificială. Între Servicii şi deservicii", în *Revista Intelligence Online*, 2018.

VASQUEZ, John, „The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition", în *The American Political Science Review*, Vol. 91, Nr. 4, 1997.

WILLIAMS, Patricia A H, MANHEKE, Rachel J., „Small Business-A Cyber Resilience Vulnerability", în *Proceedings of the 1st International Cyber Resilience Conference,* Edit. Cowan University Research Online, Perth Western, 2010.

WOLFERS, Arnold, „National Security as an Ambiguous Symbol", în *Political Science Quarterly*, Vol.67, Nr. 4, 1952, Edit. Academy of Political Science, New York, SUA, 1952.

ZAVATE, Cristian, „Angajarea țintelor teroriste. Exemplul frontului.", în *Intelligence*, Nr. 36, Serviciul Român de Informații, București, 2018, p.78.

Studii și publicații ale instituțiilor naționale / internaționale

„Președinția României la Consiliul Uniunii Europene, Coeziunea, o valoare comună europeană", https://www.romania2019.eu/wp-content/uploads/2017/11/Brosura-200x210-bilant-RO.pdf, accesat în data de 12.08.2019.

ADR, https://www.adr.gov.ro/, accesat în data de 07.01.2020.

ANCOM: Sistem Alert de avertizare în cazuri de urgență, http://www.ancom.org.ro/sistem-alert-de-avertizare-in-cazuri-de-urgenta-_5811, accesat în data de16.08.2018.

ANSPDCP, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, *„Legislație Internă*", https://www.dataprotection.ro/?page=legislatie_primara&lang=ro, accesat în data de 20.04.2019.

Banca Centrală Europeană, €CONOMIA - *The Monetary Policy Game*, http://www.ecb.europa.eu/ecb/educational/educational-games/economia/html/index.en.html, accesat în data de 21.08.2018.

Cabinetul Primului Ministru Israelian, PM Netanyahu's Remarks at the Cyber-Tech Conference, 26.06.2017;

Comisia Europeană - CoE, „2546th Council meeting - Economic and Financial Affairs" - Brussels, 25 November 2003, http://europa.eu/rapid/press-release_PRES-03-320_en.htm, accesat în data de 04.05.2019.

Comisia Europeană, „Eurobarometru de primăvară 2019: 60% dintre români au o imagine pozitivă despre UE, față de 45% media europeană", 05.08.2019, https://ec.europa.eu/romania/news/20190805_eurobarometru_primavara_ro, accesat în data de 12.08.2019.

Comisia Europeană, „European eGovernment Action Plan 2016-2020", https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020, accesat în data de 12.03.2019.

Comisia Europeană, 12.12.2018, Digital Single Market, „Artificial Intelligence: The AI4EU project launches on 1 January 2019", https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-ai4eu-project-launches-1-january-2019, accesat în data de 22.02.2019.

Comisia Europeană, ANNEX G - PADR SECURITY CLASSIFICATION GUIDE, „Security Classification Guide", Version 3.0, 14 March 2019, https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/pppa/guide/pse/pa-guide-scg-padr_en.pdf, accesat în data de 06.08.2020.

Comisia Europeană, Cécile Huet, „European Commission's Initiatives in Artificial Intelligence", https://www.oecd.org/going-digital/ai-intelligent-machines-smart-policies/conference-agenda/ai-intelligent-machines-smart-policies-huet.pdf, accesat în data de 11.08.2019.

Comisia Europeană, Comunicare a Comisiei din 19 mai 2010 către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor intitulată „O Agendă digitală pentru Europa", https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:si0016&from=RO, accesat în data de 07.03.2019.

Comisia Europeană, Digital Single Market: European Broadband Markets, https://ec.europa.eu/digital-single-market/en/download-scoreboard-reports, accesat în data de 01.04.2019.

Comisia Europeană, Înaltul Reprezentant al Uniunii pentru Afaceri Externe și Politica de Securitate, Secretariatul General al Consiliului, 6122/15, „Concluziile Consiliului privind diplomația cibernetică" din 13 septembrie 2017.

Comisia Europeană, Shared Vision, „Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy", http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accesat în data de 28.08.2020.

Congresul SUA, Cyber Diplomacy Act of 2017, 115th CONGRESS 2nd Session https://www.congress.gov/bill/115th-congress/house-bill/3776/text, accesat în data de 04.01.2018.

Consiliul Europei, „Convention on cybercrime" din 23 noiembrie 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, accesat în data de 03.03.2019.

Consiliul Europei, Adunarea Generală a ONU, New York, 27.09.2018, https://www.consilium.europa.eu/ro/meetings/international-summit/2018/09/27/, accesat în data de 14.02.2019.

Consiliul Europei, Comunicat din partea Secretariatului General al Consiliului, Bruxelles, 2017, „Atacuri cibernetice: Țările UE sunt dispuse să aplice sancțiuni ca parte a măsurilor sale pentru diplomație cibernetică", http://www.caleaeuropeana.ro/atacuri-cibernetice-tarile-ue-sunt-dispuse-sa-aplice-sanctiuni-ca-par-

te-a-masurilor-sale-pentru-diplomatie-cibernetica/, accesat în data de 19.06.2017.

Consiliul Europei, Details of Treaty No.185, „Convention on Cybercrime”, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accesat în data de 04.05.2019.

Consiliul Europei, Joint communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee Of The Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accesat în data de 13.02.2019.

Departamentul de Stat al SUA, Trezoreria SUA, Departamentul de Securitate Internă a SUA, FBI, DPRK Cyber Threat Advisory, „Guidance on the North Korean Cyber Threat”, 15.04.2020, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_cyber_threat_advisory_20200415.pdf accesat în data de 11.08.2020.

EEAS, Bruxelles, 2018, „*EU-NATO cooperation*”, https://eeas.europa.eu/sites/eeas/files/eu-nato_cooperation_factsheet.pdf, accesat în data de 30.04.2019.

EEAS, Bruxelles, 22/11/2018 - 10:55, UNIQUE ID: 170616_1, „EU-NATO cooperation - Factsheet”, https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en, accesat în data de 30.04.2019.

EEAS, Strategie globală pentru politica externă și de securitate a Uniunii Europene, http://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_ro_version.pdf, accesat în data de 04.07.2018.

ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends, ETL 2018, 2019, p.74, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, accesat în data de 20.02.2019.

ENISA, „Cyber Europe 2018: After Action Report - Findings from a cyber crisis exercise in Europe”, 2018, https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report/at_download/fullReport, accesat în data de 27.04.2019.

ENISA, „EU cybersecurity organisations agree on 2019 roadmap”, 2018, https://www.enisa.europa.eu/news/enisa-news/eu-cybersecurity-organisations-agree-on-2019-roadmap, accesat în data de 26.04.2019.

ENISA, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme, accesat în data de 22.07.2017.

Erica Moret, Patryk Pawlak, Brief SSUE, 24/2017, „The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?”, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf, accesat în data de 04.03.2019.

Federația Oamenilor de Știință Americani (FAS), „U.S. National Security Presidential Directive”, NSPD-54, https://fas.org/irp/offdocs/nspd/nspd-54.pdf, accesat în data de 10.11.2017.

Guvernul României, „Prezentarea bilanțului rezultatelor obținute de Președinția României la Consiliul Uniunii Europene în primele 100 de zile de mandat, de către prim-ministrul Viorica Dăncilă”, 17.04.2019, http://gov.ro/ro/stiri/prezentarea-bilantului-rezultatelor-obtinute-de-pre-edintia-romaniei-la-consiliul-uniunii-europene-in-primele-100-de-zile-de-mandat-de-catre-prim-ministrul-viorica-dancila&page=3, accesat în data de 12.08.2019.

http://www.pmo.gov.il/English/MediaCenter/Speeches/Pages/speechCyber260617.aspx, accesat în data de 29.11.2018.

INS, Institutul Național de Statistică, „Breviar Statistic, România în cifre”, INS 2018, http://www.insse.ro/cms/sites/default/files/field/publicatii/romania_in_cifre_breviar_statistic_1.pdf, accesat în data de 01.04.2019.

Kurt Veum, NATO NCI, „Joint Intelligence, Surveillance & Reconnaissance (JISR) in NATO”, https://fmv.se/Global/Dokument/

Nyheter%20och%20Press/2016/Sensorsymposium%202016/2_Veum_NVIA_JISR%20Initiative%20-%20Overview%20for%20SWE%20Sensors%20Conf%20(7%20Sep%202016)%20N-U.pdf, accesat în data de 12.02.2019.

MAE, Ministerul Afacerilor Externe, „Document sinteza privind politicile si programele bugetare pe termen mediu ale ordonatorilor principali de credite pentru anul 2018 si perspectiva 2019-2021", http://www.cdep.ro/pdfs/buget/2018/anexa3/Ministerul%20Afacerilor%20Externe.pdf, accesat în data de 04.03.2019.

MAE, Ministerul Afacerilor Externe, „Rolul MAE în privința securității cibernetice la nivel național", https://www.mae.ro/node/28366, accesat în data de 04.07.2018.

MAE, Ministerul Afacerilor Externe, Securitate cibernetică, „Problematica securității cibernetice în cadrul organizațiilor internaționale şi implicarea României ca membru al acestora", https://www.mae.ro/node/28369, accesat în data de 04.07.2018.

MCSI, Ministerul Comunicațiilor și Societății Informaționale, „Agenda Digitală pentru România 2020", https://www.comunicatii.gov.ro/agenda-digitala-pentru-romania-2020/, accesat în data de 04.03.2019.

MCSI, Ministerul Comunicațiilor și Societății Informaționale, „Agenda Digitală pentru România 2020", https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/Strategia-Nationala-Agenda-Digitala-pentru-Romania-2020-aprobata-feb-2015.doc, accesat în data de 04.03.2019.

MCSI, Ministerul Comunicațiilor și Societății Informaționale, „Alexandru Petrescu a discutat cu Ambasadorul Japoniei în România despre soluții privind conceptul „Societate 5.0", https://www.comunicatii.gov.ro/alexandru-petrescu-a-discutat-cu-ambasadorul-japoniei-in-romania-despre-solutii-privind-conceptul-societate-5-0/, accesat în data de 08.04.2019.

MCSI, Ministerul Comunicațiilor și Societății Informaționale, 30.08.2018, „Cloud-ul guvernamental, un beneficiu pentru instituții", https://www.comunicatii.gov.ro/cloud-ul-guvernamental-un-beneficiu-pentru-institutii/, accesat în data de 12.03.2019.

MCSI, SMART CITY Concept, https://www.comunicatii.gov.ro/smart-city-concept-2/, accesat în data de 07.01.2020.

NATO STRATCOM COE, Cyber Operations, „2007 cyber attacks on Estonia", https://www.stratcomcoe.org/download/file/fid/80772, accesat în data de 27.08.2020.

NATO, „Brussels Summit Declaration", Press Release (2018) 074 Emis în 11.07.2018, Punctul nr.2, https://www.nato.int/cps/en/natohq/official_texts_156624.htm, accesat în data de 14.07.2018.

NATO, „Collective defence - Article 5", 22.03.2017, https://www.nato.int/cps/en/natohq/topics_110496.htm, accesat în data de 03.01.2017.

NATO, „Cyber defence", 14.12.2017, https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat în data de 03.01.2017.

NATO, „Noul Concept Strategic al NATO: O perspectivă parlamentară", https://www.nato.int/docu/review/2009/0902/090203/RO/index.htm, accesat în data de 28.08.2020.

NIST, „Managing Information Security Risk: Organization, Mission, and Information System View", http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, 2011, accesat în data de 22.09.2016.

NIST, „Recommended Security Controls for Federal Information Systems and Organizations", http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, US Department of Commerce, 2009, accesat în data de 12.05.2017.

Office of the Director of National Intelligence, SUA, „2019 NATIONAL INTELLIGENCE STRATEGY" https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy, accesat în data de 28.08.2020.

ORNISS, Oficiului Registrului Național al Informațiilor Secrete de Stat, http://www.orniss.ro/ro/legislatie.html, accesat în data de 18.04.2018.

OSCE, DECISION No. 5/16 OSCE efforts related to reducing the risks of conflict stemming from the use of information and communication technologies, https://www.osce.org/cio/288086?download=true, accesat în data de 04.05.2019.

Parlamentul European, „Legislative Train Schedule - Connected Digital Single Market: Public-Private Partnerships for Cybersecurity", 20 iulie 2019, http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-public-private-partnerships-for-cybersecurity, accesat în data de 12.08.2019.

Parlamentul European, 5 July 2016, Piața Unică Europeană, „Atacurile cibernetice: UE este pregătită să reacționeze printr-o serie de măsuri care includ sancțiuni", „Commission signs agreement with cybersecurity industry to increase measures to address cyber threats", https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats, accesat în data de 04.03.2019.

U.S. Cyber Command, Vision Document as of April 2018 , https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, accesat în data de 27.11.2018.

U.S. Department of Defense, nr. NR-026-19, „New Strategy Outlines Path Forward for Artificial Intelligence", 12.02.2019.

US-CERT, Alert (TA17-132A), „Indicators Associated With WannaCry Ransomware", https://www.us-cert.gov/ncas/alerts/TA17-132A, accesat în data de 13.05.2017.

US-CERT, Alert (TA17-181A), „Petya Ransomware", https://www.us-cert.gov/ncas/alerts/TA17-181A, accesat în data de 02.07.2017.

Weiss, Gus W., The Farewell Dossier, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm, accesat în data de 14.02.2019.

Legislație

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027, https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52018SC0305&from=EN, accesat în data de 04.03.2019.

Curtea Europeană a Drepturilor Omului, Divizia Cercetare, CE, „Securitatea națională și jurisprudența Curții Europene a Drepturilor Omului", http://ier.gov.ro/wp-content/uploads/2019/06/RC-Securitatea-nationala-si-jurisprudenta-CEDO-2013.pdf.

DIRECTIVA (UE) 2016/1148 a Parlamentului European și a Consiliului *din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.*

EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0225(COD)&l=en, accesat în data de 12.03.2019.

GFCE, Report „From Awareness to Implementation", 24.10.2018, https://www.thegfce.com/documents/publications/2018/10/18/from-awareness-to-implementation, accesat în data de 30.04.2019.

Hotărâre CSAT, Art.1, „*Regulament privind organizarea și funcționarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO*", p.3, https://cert.ro/uploads/rof.pdf, accesat în data de 14.03.2019.

Hotărâre de Guvern nr. 271/2013 *pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesat în data de 21.02.2019.

Hotărâre de Guvern nr. 585 din 13 iunie 2002 *pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.*

Hotărârea de Guvern nr.494 din 02 iunie 2011 *privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.*

ISO 22301:2012, Societal security - Business continuity management systems - Requirements.

ISO 31000:2018, Risk management - Guidelines.

ISO 9001:2015, Quality management systems - Requirements.

ISO/IEC 20000-1:2011, Information technology - Service management -- Part 1: Service management system requirements.

ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC, Information technology - Security techniques - Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en, accesat în data de 18.06.2018.

Legea nr. 415 din 27 iunie 2002, *privind organizarea şi funcționarea Consiliului Suprem de Apărare a Ţării.*

Legea nr.105 din 14 aprilie 2009 *pentru ratificarea Protocolului adiţional.*

Legea nr.182 din 12 aprilie 2002, *privind protecţia informațiilor clasificate.*

Legea nr.24/2003 *pentru aprobarea Ordonanței Guvernului nr. 57/2002 privind cercetarea științifică şi dezvoltarea tehnologică.*

Legea nr.362/2018 *privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.*

Legea nr.64 din 24 martie 2004 *pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, M.Of. nr. 343/20 apr. 2004 modificată de Legea nr.105 din 14 aprilie 2009 pentru ratificarea Protocolului adiţional, adoptat la Strasbourg la 28 ianuarie 2003, la Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă şi xenofobă săvârșite prin intermediul sistemelor informatice, M.Of. nr. 278/28 apr. 2009.*

Monitorul Oficial al României.

Ordonanța Guvernului nr. 57/2002 *privind cercetarea științifică și dezvoltarea tehnologică.*

Propunere de Regulament al parlamentului european și al consiliului de instituire a programului-cadru pentru cercetare și inovare Orizont Europa și de stabilire a normelor sale de participare și de diseminare (*Text cu relevanță pentru SEE*)", http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-435-F1-RO-MAIN-PART-1.PDF, accesat în data de 04.03.2019.

Regulament al parlamentului european și al consiliului de instituire a programului Europa digitală pentru perioada 2021-2027, http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-434-F1-RO-MAIN-PART-1.PDF, accesat în data de 04.03.2019.

Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date, cu intrare în vigoare prin aplicarea directă cu data de 25 mai 2018, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EN, accesat în data de 28.06.2018.

RFC 2350 description for CERT-RO, p.3, https://cert.ro/vezi/document/RFC2350-CERT-RO, accesat în data de 14.03.2019.

Strategia de securitate cibernetică a României, https://www.mae.ro/node/28367, accesat în data de 14.03.2019.

Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52013JC0001&from=ro, accesat în data de 21.02.2019.

Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024 cu nr. DSN 1/794 din 26.05.2020, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accesată în data de 11.08.2020.

Tratatul de instituire a Comunității Europene a Cărbunelui şi Oțelului (CECO), https://eur-lex.europa.eu/eli/treaty/ceca/sign, accesat în data de 30.08.2020.

Alte studii și publicații

AGERPRES, https://www.agerpres.ro/externe/2017/06/19/ue-a-convenit-sa-impuna-sanctiuni-hackerilor-care-ataca-retele-informatice-ale-statelor-membre-13-19-19, accesat în data de 04.03.2019.

AMITAI, Ofer, PortNox, „Why is It So Easy to Hack an IP Security Camera and Any IoT Device?”, 2018, https://www.portnox.com/blog/iot/why-is-it-so-easy-to-hack-an-ip-security-camera-and-any-iot-device/, accesat în data de 23.04.2019.

ANDERSON, R., SCHNEIER, B., „Economics of Information Security, IEEE SECURITY & PRIVACY”, https://www.schneier.com/academic/paperfiles/paper-economics.pdf, accesat în data de 18.04.2019.

ANDREESCU, Crişan, „Klaus Iohannis, Facebook. Cine este omul din spatele președintelui ales care i-a adus peste un milion de

fani”, 20 noi 2014, https://www.dcnews.ro/klaus-iohannis-facebook-cine-este-omul-din-spatele-pre-edintelui-ales-care-i-a-adus-peste-un-milion-de-fani_460018.html, accesat în data de 14.07.2018.

BACHNER, Michael, „At UN, Netanyahu reveals Iranian nuclear warehouse, urges IAEA to go inspect it”, https://www.timesofisrael.com/netanyahu-reveals-secret-iranian-nuclear-warehouse-in-un-speech/, accesat în data de 14.02.2019.

Bitdefender, „Detectați atacurile de tip exploit și zero-day”, https://www.bitdefender.ro/business/usecases/exploits-zero-days.html, accesat în data de 27.11.2018.

Bitdefender, „Zece predicții despre atacurile cibernetice din 2019”, 10.12.2018, https://www.bitdefender.ro/news/zece-predic%EF%BF%BD%EF%BF%BDii-despre-atacurile-cibernetice-din-2019-3607.html, accesat în data de 07.03.2019.

BOND, David, „Seven UK banks targeted by co-ordinated cyber attack”, 25.04.2018, https://www.ft.com/content/2e582594-48ab-11e8-8ee8-cae73aab7ccb, accesat în data de 14.02.2019.

BROWN , Gary, YUNG, Christopher D., „Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity”, 19 ianuarie 2017 https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/, accesat în data de 29.11.2018.

BUMILLEr, Elisabeth, „Panetta Warns of Dire Threat of Cyberattack on U.S.”, Jurnalul The New York Times din 11.10.2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html, accesat în data de 21.11.2018.

BURT, Tom, 20.02.2019, „New steps to protect Europe from continued cyber threats”, https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/, accesat în data de 07.03.2019.

BUTU, Alina Grigoraș, “WannaCry” ransomware attack: Romania the 9th most affected country, securelist.com says. Dacia Miove-

ni plant's IT system failed, 13.05.2017, https://www.romaniajournal.ro/wannacry-ransomware-attack-romania-the-9th-most-affected-country-securelist-com-says-dacia-mioveni-plants-it-system-failed/, accesat în data de 15.02.2019.

CASAL, Julio, „1.4 Billion Clear Text Credentials Discovered in a Single Database”, 8 decembrie 2017, https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14, accesat în data de 03.01.2017.

Christo Petrov, „Big Data Statistics 2019”, 22.03.2019, https://techjury.net/stats-about/big-data-statistics/, accesat în data de 11.08.2019.

CILEACU, Cristina, „Estonia, avansată în era digitalizării”, în emisiunea *Pașaport diplomatic*, 29.05.2020, https://www.youtube.com/watch?v=cFMyF1__WNA, accesat în data de 12.08.2020.

CISCO, „Cisco 2015 Annual Security Report”, https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf, accesat în data de 15.08.2016.

CISCO, Raportul Anual de Securitate Cibernetică, CISCO 2017, Ianuarie 2017, Europe Headquarters, Cisco Systems International BV Amsterdam, The Netherlands.

COLDEA, Florian, „Securitatea cibernetică, de la „perla coroanei“ în IT spre „business as usual“ în societate”, https://intelligence.sri.ro/securitatea-cibernetica-de-la-perla-coroanei-spre-business-usual-societate/, accesat în data de 29.07.2019.

CORERA, Gordon, BBC News, „Rapid escalation of the cyber-arms race”, 29.04.2015, https://www.bbc.com/news/uk-32493516, accesat în data de 04.12.2018.

COSEGLIA, Jared, LegatTech News, „Unit 8200 CEO takes accelerated learning to the cyber masses”, 16 ianuarie 2018, https://trustaffingpartners.com/uploaded/articles/Unit%208200.pdf, accesat în data de 29.11.2018.

COUGHLAN, Sean, „Top university under ‚ransomware' cyber-attack", http://www.bbc.com/news/education-40288548, accesat în data de 15.06.2017.

CRERAR, Pippa, HENLEY, Jon, WINTOUR, Patrick, „Russia accused of cyber-attack on chemical weapons watchdog", 04.10.2018, https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body, accesat în data de 15.02.2019.

CROWE, Jonathan, Must-Know Ransomware Statistics 2017, „Stats & Trends", Iunie 2017, https://blog.barkly.com/ransomware-statistics-2017, accesat în data de 24.12.2017.

CyberTech, The event for cyber industry, https://www.cybertechisrael.com/cybertech-tlv-2017, accesat în data de 29.11.2018.

DARAGAHI, Borzou, TRIEST, Vincent, Independent, 08.12.2018, „NATO nation Albania publicly posting sensitive intelligence data online -'By getting into Albania's system they can get into NATO's system'", https://www.independent.co.uk/news/world/europe/albania-intelligence-data-posted-online-nato-defence-military-finance-security-a8672446.html, accesat în data de 11.08.2019.

DENNISON, Susi, Ulrike Esther Franke, & Paweł Zerka, ECFR, 2018, „The nightmare of the dark: The security fears that keep europeans awake at night", https://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n#, accesat în data de 11.08.2019.

Diplomacy.edu, „Big data: The next accelerator for diplomacy?", https://www.diplomacy.edu/blog/big-data-next-accelerator-diplomacy, accesat în data de 16.08.2018.

DUMITRESCU, Lucian, „Lansarea Barometrului Culturii de Securitate. Ce este Cultura de Securitate?", 12.04.2018, https://larics.ro/lansarea-barometrului-culturii-de-securitate-ce-este-cultura-de-securitate/, accesat în data de 22.07.2019.

ERMAN, Marko, „Launch f First European Artificial Intelligence Platform Coordinated By Thales", 01.10.2019, https://www.thalesgroup.com/en/group/journalist/press-release/launch-first-european-artificial-intelligence-platform-coordinated, accesat în data de 22.02.2019.

EROUKHMANOFF, Clara, „Securitisation Theory: An Introduction", E-International Relations Students, 14.01.2018, https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/, accesat în data de 21.11.2018.

FIELD, Matthew, „WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled", 11.10.2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/, accesat în data de 14.02.2019.

FireEye, Advanced Persistent Threat Groups, „Who's who of cyber threat actors", https://www.fireeye.com/current-threats/apt-groups.html, accesat în data de 29.11.2018.

FOXX, Chris, „NHS cyber-attack: GPs and hospitals hit by ransomware", http://www.bbc.com/news/health-39899646, accesat în data de 13.05.2017.

George GMT, „Lansarea primei platforme de Inteligență Artificială la nivel european, în coordonarea Thales", 20.02.2019, https://www.rumaniamilitary.ro/lansarea-primei-platforme-de-inteligenta-artificiala-la-nivel-european-in-coordonarea-thales, accesat în data de 22.02.2019.

GILLETT, Frank E., MCCARTHY, John C., „Predictions 2015: Software Platforms Drive Internet-Of-Things Adoption", https://www.forrester.com/Predictions+2015+Software+Platforms+Drive+InternetOfThings+Adoption/fulltext/-/E-res119422, accesat în data de 27.07.2016.

GReAT, „WannaCry ransomware used in widespread attacks all over the world", 12.05.2017 https://securelist.com/wannacry-ran-

somware-used-in-widespread-attacks-all-over-the-world/78351/, accesat în data de 15.02.2019.

GRIGORESCU, Denis, , „Cum a depistat Facebook ‚laboratorul de troll' al PSD", în Ziarul *Adevăru*l, 12.03.2019

GSMA, Raportul anual GSMA Intelligence, „Market Overview Report 2019", https://www.gsmaintelligence.com/markets/2859/dashboard/, accesat în data de 11.04.2019.

GSMA, Raportul anual GSMA, „The Mobile Economy 2019", https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download, accesat în data de 12.04.2019.

HA, Mathew, MAXWELL, David, *Kim Jong Un's ‚All-Purpose Sword' North Korean Cyber-Enabled Economic Warfare*, Edit. FDD PRESS, Washington, DC, SUA, 2018.

Heidelberg Institute for International Conflict Research, Conflict Barometer 2017, „Global Conflict Panorama: Interstate Conflict Constellations 2012, 2014, and 2017", https://hiik.de/conflict-barometer/current-version/?lang=en, accesat în data de 09.12.2018.

ILASCU, Ionut, „Rogue GSM Towers and Internet of Things Devices", 2018, https://www.bitdefender.com/box/blog/iot-news/rogue-gsm-towers-internet-things-devices/, accesat în data de 23.04.2019.

ISACA, CMMI Institute, „A risk-aware path to cybersecurity resilience and maturity", 2018, https://cmmiinstitute.com/getattachment/8d1133ac-4050-4ad0-9273-e4c43d356f06/attachment.aspx, accesat în data de 04.03.2019.

JIANG, Henry, „The Map of Cybersecurity Domains (version 1.0)", 10.02.2017, https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/, accesat în data de 03.05.2019.

KANNO-YOUNGS , Zolan, PERLROTH, Nicole, „Iran's Military Response May Be 'Concluded,' but Cyberwarfare Threat

Grows", 08.01.2020, https://www.nytimes.com/2020/01/08/us/politics/iran-attack-cyber.html, accesat în data de 11.08.2020.

Kaspersky, „*Kaspersky Security Bulletin: Story of the year 2017*", pp.5-8, https://cdn.securelist.com/files/2017/11/KSB_Story_of_the_Year_Ransomware_FINAL_eng.pdf, accesat 24.12.2017.

KHOSROWSHAHI, Dara, Uber Newsroom, „*2016 Data Security Incident*", https://www.uber.com/newsroom/2016-data-incident/, accesat 23.04.2019

KLECZYNSKI, Marcin, „A Look At The Five Biggest Future Cyberthreats Of 2018", https://www.forbes.com/sites/forbestechcouncil/2018/01/02/a-look-at-the-five-biggest-future-cyberthreats-of-2018/#1861a9b149d2, accesat în data de 05.01.2018.

KRASIMIROV, Angel, TSOLOVA, Tsvetelia, REUTERS, 16.07.2019, „*In systemic breach, hackers steal millions of Bulgarians' financial data*", https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-hit-bulgaria-send-data-from-russian-email-government-idUSKCN1UB0MA, accesat 11.08.2019.

KURBALIJA, Jovan, DIPLO, 04.11.2016, „*25 Points for Digital Diplomacy*", https://www.diplomacy.edu/blog/25-points-digital-diplomacy, accesat 11.08.2019.

LIPTA, Andrew, The Verge, 25.05.2019, „*Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems*", https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity, accesat 11.08.2019.

LOMAS, Natasha, TechCrunch, „*Venezuela claims drones loaded with explosives used in failed attack on president*", https://techcrunch.com/2018/08/05/venezuela-claims-drones-loaded-with-explosives-used-in-failed-attack-on-president/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=LfUMR7bPwJbLbb-Mm5hMzQ, accesat 23.04.2019.

LUPITU, Robert, „Klaus Iohannis și Shinzo Abe, anunț de la Tokyo: Parteneriatul Strategic dintre România și Japonia va fi lansat în 2021, la 100 de ani de la stabilirea relațiilor diplomatice", https://www.caleaeuropeana.ro/klaus-iohannis-si-shinzo-abe-anunt-de-la-tokyo-parteneriatul-strategic-dintre-romania-si-japonia-va-fi-lansat-in-2021-la-100-de-ani-de-la-stabilirea-relatiilor-diplomatice/, accesat în data de 07.06.2020.

LUPITU, Robert, „Ministrul Comunicațiilor, vizită în SUA. Alexandru Petrescu s-a întâlnit cu consilierul lui Donald Trump pentru politica de securitate cibernetică a Statelor Unite", https://www.caleaeuropeana.ro/ministrul-comunicatiilor-vizita-in-sua-alexandru-petrescu-s-a-intalnit-cu-consilierul-lui-donald-trump-pentru-politica-de-securitate-cibernetica-a-statelor-unite, accesat în data de 07.08.2019.

LUPITU, Robert, „Secretarul general al NATO atrage atenția privind alocarea a 2% din PIB pentru Apărare de către România: "Sper că veți reuși să astupați acest gol"", https://www.caleaeuropeana.ro/secretarul-general-al-nato-atrage-atentia-privind-alocarea-a-2-din-pib-pentru-aparare-de-catre-romania-sper-ca-veti-reusi-sa-astupati-acest-gol/, accesat în data de 12.08.2019.

MARTIN, Ben, TITCOMB, James, „Regulators could fine Tesco Bank over cyber attack", 07.11.2016, https://www.telegraph.co.uk/business/2016/11/07/tesco-bank-to-freeze-customer-transactions-after-hacking-attack/, accesat în data de 13.02.2019.

McAfee Labs din 2015 - Threats Predictions, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf, accesat în data de 21.05.2017.

McAfee, Raportul anual de predicție a amenințărilor McAfee Labs din 2015 http://www.mcafee.com/;

MCCARTHY, Justin, „Americans Cite Cyberterrorism Among Top Three Threats to U.S.", 10.02.2016, https://news.gallup.com/

poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx, accesat în data de 21.11.2018.

MEDIAFAX, Interviu din 03.03.2019 pentru MEDIAFAX cu ministerul MCSI, domnul Alexandru Petrescu, https://www.mediafax.ro/economic/interviu-ministrul-comunicatiilor-intentia-e-sa-avem-licitatia-pentru-5g-in-2019-ce-spune-despre-oug-114-17896378, accesat în data de 12.03.2019.

Most famous social network sites worldwide as of July 2018, ranked by number of active users (in millions), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/, accesat în data de 27.08.2018.

MULRINE, Anna, „How North Korea built up a cadre of code warriors prepared for cyberwar", 06.02.2015, https://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar, accesat în data de 29.11.2018.

POGUE, Chris, „The Black Report", 2016, https://www.nuix.com/sites/default/files/report_the_black_report_web_us.pdf, accesat în data de 03.01.2017.

POSIRCA, Ovidiu, „Dacia production in Romania, partially crippled by cyber-attack | WannaCry infection suspected", 13.05.2017, http://business-review.eu/news/dacia-production-in-romania-partially-crippled-by-cyber-attack-wannacry-infection-suspected-137678, accesat în data de 13.02.2019.

PRAKASH Binwal, „Creating a Cybersecurity Governance Framework: The Necessity of Time", iulie 2015, https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/, accesat în data de 22.10.2017.

RADU, Răzvan Horaţiu, Conferinţa Internaţională: Rolul justiției constituționale în protecţia valorilor statului de drept, Manifestare dedicată celei de-a 20-a aniversări a Constituției Republicii Moldova, „*Prioritatea ordinii juridice UE asupra dreptului*

național", Chișinău, 8-9 septembrie 2014, http://www.constcourt.md/public/files/file/conferinta_20ani/programul_conferintei/Razvan_Horatiu_Radu.pdf, accesat în data de11.03.2019.

RAGAN, Steve, SCO, „Researcher says Adult Friend Finder vulnerable to file inclusion vulnerabilities", 2016, https://www.csoonline.com/article/3132533/researcher-says-adult-friend-finder-vulnerable-to-file-inclusion-vulnerabilities.html, accesat în data de 23.04.2019.

RANGER, Steve, „Inside the secret digital arms race: Facing the threat of a global cyberwar", 12.09.2018, https://www.techrepublic.com/article/inside-the-secret-digital-arms-race/, accesat în data de 04.12.2018.

SALAMONE, Salvatore, „2020 Will Be the Year of Continuous Intelligence", 2020, https://www.rtinsights.com/2020-will-be-the-year-of-continuous-intelligence/, accesat în data de 07.01.2020.

SATTLER, Jason, „Threats & Research IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks", https://blog.f-secure.com/iot-threats/, 2019, accesat în data de 23.04.2019.

SCHARRE, Paul, „Killer Apps:The Real Dangers of an AI Arms Race", https://www.foreignaffairs.com/articles/2019-04-16/killer-apps?utm_campaign=site_visitor.unpaid.engagement&utm_source=facebook&utm_medium=tr_social&utm_content=72332040&_hsenc=p2ANqtz--65C7cpVxdnBIfZ5_OY-itxxPkXskZDGq8mqNC0NlU0VeCbGZ2HNzuqH8G1fgZVTXEOnbBUim9wMQMS795xlW7fNAoMHLhYnZfOWaN8SddXeczUng&_hsmi=72332042&fbclid=IwAR0IbYfieSRq03n9ZWrvmJhDgr-rkXRLM1dyMOXPy2gkb5DKYp-WROiutdk, accesat în data de 04.05.2019.

SHARWOOD, Simon, „A USB stick as a file server? We've done it!", 2016 https://www.theregister.co.uk/2016/08/26/a_usb_stick_as_a_file_server_weve_done_it/, accesat în data de 23.04.2019.

SISENSE, „Augmented Analytics: the Future of Business Intelligence", https://pages.sisense.com/rs/601-OXE-081/images/Augmented%20Analytics%20The%20Future%20of%20Business%20Intelligence.pdf, accesat în data de 07.01.2020.

SKOV, Anders, The Center for Digital Generation, „Digital Dannelse, The Digital Competence Wheel", Copenhaga, 2016, https://digital-competence.eu/front/what-is-digital-competence/, accesat în data de 01.04.2019.

SLY, Liz, „U.S. soldiers are revealing sensitive and dangerous information by jogging", 29.01.2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?noredirect=on&utm_term=.c3748d111f92, accesat în data de 03.05.2019.

SOLOMON, Jay, U.S. Detects Flurry of Iranian Hacking, „American officials say they believe cyberattacks tied to arrest in Tehran of Iranian-American businessman", 4 noiembrie 2015, https://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754, accesat în data de 03.12.2018.

STAFF, Toi, „TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet", 31.10.2018, https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/, accesat în data de 14.02.2019.

Symantec, 2015 Internet Security Threat Report, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, accesat în data de 21.05.2017;

The Guardian Press Association, „Tesco Bank fined £16.4m by watchdog over cyber-attack”, https://www.theguardian.com/business/2018/oct/01/tesco-bank-fined-cyber-attack-fca, accesat în data de 13.02.2019.

Varonis, „Data Under Attack: 2018 Global Data Risk Report from The Varonis Data Lab”,https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf, accesat în data de 23.04.2019.

VOLODZKO, David, „Marriott Breach Exposes Far More Than Just Data”, 04.12.2018, https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#1f91929d6297, accesat în data de 30.04.2019.

WHITE, Hannah, IoT For All, „Voice Assistants Are Taking Over Consumer IoT”, 2019, https://www.iotforall.com/voice-assistants-consumer-iot/, accesat în data de 23.04.2019.

ZETTER, Kim, WIRED, „That insane, $81m Bangladesh bank heist? Here's what we know”, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/, accesat în data de 23.04.2019.

Surse electronice

Archive.org, https://archive.org/

Center for a New American Security, https://www.cnas.org/

Centrul de Resurse pentru Furtul de Identitate, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf, accesat în data de 23.04.2019.

CISCO, Benchmark Study, „Anticipating the Unknowns”, https://ebooks.cisco.com/story/anticipating-unknowns#!/page/1, accesat în data de 23.04.2019.

DEF CON 25, 27-30 iulie 2017, https://www.defcon.org/html/defcon-25/dc-25-index.html, accesat în data de 04.08.2017.

DLA Piper, „GDPR Data Breach Survey:February 2019", https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf?la=-de&hash=C9DD3CB559E5F8E47E395FBB175F6965A15F771F, accesat în data de 30.04.2019.

ESRI, https://www.esri.com

EU GDPR.org , „Site Overview", https://www.eugdpr.org/, accesat în data de 03.01.2017.

Gazetă On-Line CNBC, The Internet of Things, http://www.cnbc.com/id/101411902, accesat în data de 21.05.2017.

GFCE, Global Forum on Cyber Expertise, https://www.thegfce.com/

Google Ideas. DDoS data ©2013, Arbor Networks, Inc., http://www.digitalattackmap.com/#anim=1&color=0&country=RO&list=0&ti-me=17796&view=map, accesat în data de 09.12.2018.

Grey Literature Report, http://www.greylit.org/about

Harvard Kenedy School, Belfer Center, https://www.belfercenter.org

IBM Corp. (2017), IBM SPSS Statistics for Windows, Version 25.0, Armonk, NY: IBM Corp, https://www-01.ibm.com/support/doc-view.wss?uid=swg24043678 accesat în data de 19.03.2019.

IBM i2 Analyst's Notebook Release Notes, https://www-01.ibm.com/support/docview.wss?uid=swg27036288

ICANN, https://www.icann.org

IEEE.org IEEE Xplore Digital Library, https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=security%20AND%20resilience%20, accesat în data de 21.11.2016.

International Telecommunication Union, https://www.itu.int/

Internet World Stats, „*World internet usage and population statistics*", iunie 2019 https://www.internetworldstats.com/stats.htm, accesat în data de 29.07.2019.

IT Governance Ltd, https://www.itgovernance.co.uk/cyber-resilience

JSTORE, http://www.jstor.org

Lori M. Cameron, „What is cloud computing? Seven years later, has the time come to officially redefine it?", 24.07.2018, https://publications.computer.org/cloud-computing/2018/07/24/cloud-computing-definition-nist/, accesat în data de 26.07.2018.

LycaMobile, https://www.lycamobile.ro/ro/, accesat în data de 11.04.2019.

Microsoft, Win32/Locky, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Locky, accesat în data de 10.01.2018.

Ofelia Hobincu, „*Caracteristicile informaţiei*", martie 2008, http://www.perfect-service.ro/intelinet/2008/martie/intel%28i%29net.php?legatura=2, accesat în data de 19.06.2016.

Open Grey, http://www.opengrey.eu/about/greyliterature

OSTI, Office of Scientific and Technical Information, https://www.osti.gov

PWNTHECODE, „*Despre pentesting*", https://pwnthecode.com/courses/web-application-pentesting-101/despre-pentesting, accesat în data de 02.05.2019.

Research Gate, https://www.researchgate.net/

Ronald van Loon, „What Is the Future of Data Warehousing?", 18.09.2016, https://mapr.com/blog/what-future-data-warehousing/, accesat în data de 12.05.2018.

RT, Russia Today, https://www.rt.com/

SAGE Journals, https://journals.sagepub.com

Schneier on Security, https://www.schneier.com

Spluk.com, Press Release, 2018, https://www.splunk.com/en_us/newsroom/press-releases/2018/telstra-delivers-personalized-customer-experience-with-splunk.html, accesat în data de 11.08.2019.

Stanford University, http://stanford.edu

STRAVA, Baza Militară de la Deveselu, Jud. Olt, 03.05.2019, https://www.strava.com/heatmap#14.04/24.38239/44.07120/hot/all, accesat în data de 03.05.2019.

Symantec, Internet Security Threat Report, Vol.23 http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_, accesat în data de 23.04.2019.

Telstra, „*Telstra Global Services Practice*", https://www.telstra.com.au/content/dam/tcom/business-enterprise/consulting-services/pdf/telstra-global-services-capabilities.pdf, accesat în data de 11.08.2019.

The MIT Press, https://www.mitpressjournals.org

The University of Chicago, http://mearsheimer.uchicago.edu

UC San Diego, http://pages.ucsd.edu

Under the Armor, Press Release, „Under Armour Notifies MyFitnessPal Users Of Data Security Issue", http://investor.underarmour.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue?ReleaseID=1062368, accesat în data de 23.04.2019.

University of Helsinki, HELDA, https://helda.helsinki.fi/

US Federal Science, https://www.science.gov/scigov/

Varonis, „Data Under Attack: 2018 Global Data Risk Report from The Varonis Data Lab", https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf, accesat în data de 23.04.2019.

WikiLeaks, https://search.wikileaks.org

Wikistrat, http://www.wikistrat.com/

Wilson Center.org, https://www.wilsoncenter.org/

Yahoo! Help, „Yahoo 2013 Account Security Update FAQs", https://help.yahoo.com/kb/account/SLN28451.html?impressions=true, accesat în data de 23.04.2019.

Youtube, canal #VICEonHBO, „How Israel Rules The World Of Cyber Security | VICE on HBO" https://www.youtube.com/watch?v=ca-C3voZwpM, accesat în data de 29.11.2018.

Zingbox, White Paper, „*Discovery of Cyberattack Trends Targeting Connected Medical Device - Detailed analysis of hackers leveraging device error messages*", http://go.zingbox.com/rs/562-ZPO-907/images/Zingbox_Medical_Device_Cyberattack_Trend_Report.pdf, accesat în data de 23.04.2019.

Zotero, https://www.zotero.org/

Lista figurilor

Figura nr.1. Distribuția participanților: Autopercepția corespondenților pe gradul de competențe digitale. 347
Figura nr.2. Distribuția participanților care au urmat cursuri în domeniu informatic și a celor care nu au urmat astfel de cursuri, separat în funcție de statutul socio-economic. Procentele au fost calculate din totalul răspunsurilor valide. 348
Figura nr.3. Distribuția numărului de ore petrecut utilizând tehnologia digitală (a) și a proporției din timp petrecut online (b). Liniile verticale corespund percentilelor 25 și 75. 349
Figura nr.4. Distribuția importanței tehnologiei digitale în funcție de mediul de proveniență al participanților. Procentele afișate au fost calculate din totalul răspunsurilor valide.. 351
Figura nr.5. Distribuția importanței tehnologiei digitale în funcție de statutul socio-economic al participanților. Procentele au fost calculate din totalul răspunsurilor valide. 352
Figura nr.6. Distribuția utilizatorilor care au auzit și a celor care nu au auzit despre securitate informatică în funcție de statutul socio-economic al acestora. Procentele sunt calculate din totalul cazurilor valide. . 360
Figura nr.7. Distribuția importanței percepute a securității informatice în funcție de nivelul competențelor digitale ale utilizatorilor. Procentele sunt calculate din totalul cazurilor valide. 361
Figura nr.8. Distribuția celor care subscriu cu adresa de e-mail diferitelor cauze, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide. 363

Figura nr.9. Distribuția celor care răspund mesajelor, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide. 364
Figura nr.10. Distribuția celor care au divulgat prin constrângere parole sau conturi de acces, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide. 365
Figura nr.11. Distribuția celor care au în lista lor de contacte persoane pe care nu le cunosc, în funcție de statutul socio-economic. Procentele afișate sunt calculate din totalul răspunsurilor valide.. 366
Figura nr.12. Modificările suferite de informație în ciclul de viață al acesteia 81
Figura nr.13. Piramida lui Maslow 112
Figura nr.14. Managementul riscului de securitate din sistemele informaționale. 115
Figura nr.15. Corespondența dintre nivelurile de risc și acceptabilitatea acestora ca elemente fundamentale ale managementului riscului și al securității. 116
Figura nr.16. Corelarea elementelor ce asigură minimizarea riscului în organizație 120
Figura nr.17. Raportul anual privind conflictele la nivel global *„Global Conflict Panorama, Interstate Conflict Constellations 2012, 2014, and 2017"186*
Figura nr.18: *Simulare în timp real a ~1% din atacurile de tip DDOS la nivel global, „Digital Attack Map" din data de 22 septembrie 2018, ora 18:00 . 187*
Figura nr.19. Grafic privid rezultatele aduse de Diplomația cibernetică în raport cu Diplomația publică / consulară 243
Figura nr.20. Cele mai renumite instrumente de socializare online din întreaga lume (iulie 2018), reprezentate în baza numărului de utilizatori activi (în milioane) 257
Figura nr.21. Diagrama sistemului de securitate cibernetică al UE 314

Lista tabelelor

Tabelul nr.1 - Metode, tehnici, procedee și instrumente de cercetare utilizate . . . 27
Tabelul nr.2 - Tabel de contingență . . . 343
Tabelul nr.3. Procentele de utilizare ale echipamentelor digitale în funcție de variabilele socio-demografice. Procentele sunt calculate din totalul participanților din fiecare categorie de echipament digital. . . . 353
Tabelul nr.4. Distribuția scopului utilizării echipamentelor digitale în funcție de variabilele socio-demografice. Procentele sunt calculate din totalul participanților din fiecare categorie a variabilelor socio-demografice. . . . 355
Tabelul nr.5. Viziune asupra raportului anarhie-încredere din prisma celor trei școli de gândire . . . 191
Tabelul nr.6. Reziliența cibernetică expusă pe șase nivele. . . . 282
Tabelul nr.7. Evenimentele cibernetice adverse . . . 283
Tabelul nr.8. Caracteristicile securității cibernetice în raport cu reziliența cibernetică . . . 284

Anexe

Nota autorului: Toate datele și informațiile prezentate în textul tezei au fost culese ***exclusiv*** din surse deschise de informații. Unele referințe bibliografice au făcut obiectul unor scurgeri de informații clasificate aparținând unor terțe entități guvernamentale, acestea au fost preluate și amintite pe parcursul acestei lucrări strict din rațiuni de cercetare științifică. Interpretarea valorii intrinseci a celor prezentate în cadrul anexelor a fost realizată cu maximă precauție, sub rezerva unor documente a căror credibilitate este dificil de verificat și evaluat propriu-zis.

ANEXA NR.1.
Chestionar „Cultura de securitate cibernetică în România"

Sex: F ☐ **M** ☐ **Vârstă** ☐ **ani**

Mediul de proveniență: RURAL ☐ **URBAN** ☐

1. Care este statutul dumneavoastră social?

☐ Elev, specializarea ______

☐ Student, specializarea ______

☐ Angajat

☐ Antreprenor / Liber profesionist

☐ Șomer / fără ocupație

☐ Pensionar

2. Care este nivelul dumneavoastră în competențe digitale *(utilizarea tehnologiei informatice: calculator, laptop, tabletă etc)*:

☐ Începător

☐ Mediu

☐ Avansat

3. Ați urmat vreodată cursuri în domeniul informatic?

DA ☐ NU ☐

4. Ce echipamente digitale utilizați?

☐ Calculator

☐ Laptop

☐ Tabletă

☐ Smartphone

☐ Altele, precizați care: ______

5. În ce scop utilizați tehnologia informatică:

☐ Profesional

☐ Dobândirea informațiilor

☐ Socializare

☐ Achiziții și servicii online
☐ Corespondență
☐ Relaxare/Distracție
☐ Altele, precizați care ______

6. Precizați câte ore pe zi petreceți utilizând tehnologia digitală:
☐ ore, din care online ☐ ore.

7. Utilizați aplicații informatice?
DA ☐ NU ☐
Dacă ați răspuns cu **DA**, care sunt acestea?

8. Cât de importantă este pentru dumneavoastră tehnologia digitală?
☐ Deloc importantă
☐ Puțin importantă
☐ Destul de importantă
☐ Importantă
☐ Foarte importantă

9. Ați auzit despre expresia "*Securitate informatică*"?
DA ☐ NU ☐
Descrieți în câteva propoziții la ce credeți că se referă:

______

10. Cât de importantă este securitatea informatică pentru dumneavoastră?
☐ Deloc importantă
☐ Puțin importantă
☐ Destul de importantă
☐ Importantă
☐ Foarte importantă

11. Vi s-a întâmplat să vorbiți despre aspecte din viața dvs. personală cu persoane necunoscute?

DA ☐ NU ☐

12. Ați susținut diferite cauze umanitare, sociale, proiecte prin subscriere cu emailul dvs.?

DA ☐ NU ☐

13. Ați susținut cu sume mici de bani diferite campanii umanitare, sociale etc?

DA ☐ NU ☐

14. Ați încredințat date personale (*de exemplu date din C.I., CNP, adresă, imagini, înregistrări audio sau video*) unor persoane străine în farmacii, în promoții din magazine, concursuri online, promoteri, etc?

DA ☐ NU ☐

15. Ați oferit de bunăvoie copii după documente personale (*certificat naștere, căsătorie, C.I. etc*)?

DA ☐ NU ☐

16. Prin constrângere ați oferi

DA ☐ NU ☐

☐ Documente personale (*carte identitate, certificat naștere, căsătorie etc.*)

☐ Parole/Conturi de acces

☐ Informații cu caracter confidențial

17. Vi s-a solicitat vreodată ajutorul sau ați cerut dvs. ajutorul pentru utilizarea unui card bancar?

DA ☐ NU ☐

18. Aveți în lista dvs. de contacte persoane pe care nu le cunoașteți?

DA ☐ NU ☐

19. Aveți conturi online pe care le utilizați împreună cu altcineva?

DA ☐ NU ☐

20. Ați primit vreodată mesaje pe telefon sau pe email prin care ați fost înștiințat că ați câștigat un premiu sau o sumă de bani, fără să fi participat la vreo formă de concurs sau tombolă?

DA☐ NU☐

21. În cazul în care ați răspuns cu DA, cum ați acționat în continuare?

☐ Am deschis mesajul, email-ul;
☐ Am răspuns mesajului, email-ului;
☐ Am urmat instrucțiunile din mesaj, email;
☐ Am șters mesajul.

22. Ați fost vreodată victimă a unei infracțiuni informatice?

DA ☐ NU ☐

23. Dacă DA, bifați tipul de infracțiune:

☐ Furt de date personale
☐ Furt de identitate
☐ Virusarea sistemului informatic (*modificarea sau ștergerea datelor*)
☐ Altele, precizați care: ______

24. Aveți în cercul dvs. de cunoștințe persoane care au fost victime ale unor infracțiuni informatice?

DA ☐ NU ☐

25. Descrieți în câteva cuvinte cum ați reacționa dacă v-ați afla în postura de victimă a unei infracțiuni informatice?

26. Considerați că România este pregătită pentru un eventual val de atacuri informatice?

DA ☐ NU ☐

Motivați răspunsul dumneavoastră:

27. Cât de importantă considerați introducerea studiului "*Securității informatice*" în:

MEDIUL PREUNIVERSITAR:	MEDIUL UNIVERSITAR:
☐ Deloc importantă	☐ Deloc importantă
☐ Puțin importantă	☐ Puțin importantă
☐ Destul de importantă	☐ Destul de importantă
☐ Importantă	☐ Importantă
☐ Foarte importantă	☐ Foarte importantă

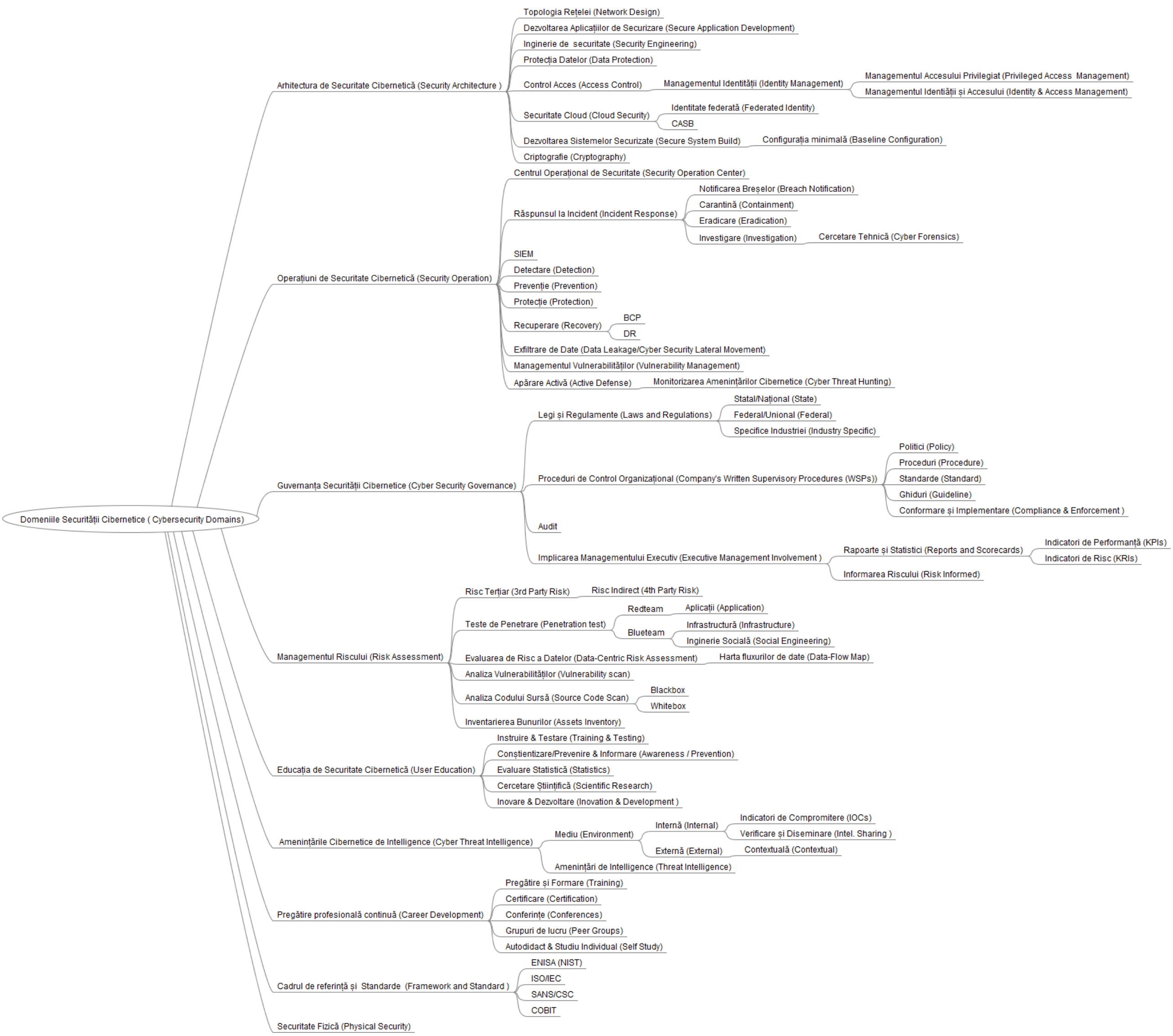
Motivați răspunsul dumneavoastră:

ANEXA NR.2.
Macheta centralizatoare pentru chestionarul
„Cultura de securitate cibernetică în România"

INDEX	ÎNTREBA-RE	CORESPONDENT	V.1	V.2	V.3	V.4	V.5	V.6	V.7
1	Cod Chesti-onar	ID	X						
2	I.0.1	Sex	X	X					
3	I.0.2	Varsta	X	X					
4	I.0.3	mediu_prov	X	X					
5	I.1.1	Specializare	X						
6	I.1.2	statut_social		X	X	X	X		
7	I.2	comp_digitale	X	X	X				
8	I.3	cursuri_info	X	X					
9	I.4.1	echipam_digitale 1	X						
10	I.4.2	echipam_digitale 2		X					
11	I.4.3	echipam_digitale 3			X				
12	I.4.4	echipam_digitale 4				X			
13	I.4.5	echipam_digitale 5					X		
14	I.4.6	ech_digitale_altele					X		
15	I.5.1	techn_scop 1	X						
16	I.5.2	techn_scop 2		X					
17	I.5.3	techn_scop 3			X				
18	I.5.4	techn_scop 4				X			
19	I.5.5	techn_scop 5					X		
20	I.5.6	techn_scop 6						X	
21	I.5.7	techn_scop 7							X
22	I.5.8	tech_scop_altele							X
23	I.6.1	ore_util_tech_total	X						
24	I.6.2	ore_util_tech_onlne		X					
25	I.7.1	util_aplicatii_info	X						
26	I.7.2	util_aplicatii_info_care		X					
27	I.8	imp_tech	X	X	X	X	X		
28	I.9.1	expr_sec_info	X	X					
29	I.9.2	sec_info_descriere	X						

30	I.10	imp_sec_info	X	X	X	X	X		
31	I.11	detalii_pers_straini	X	X					
32	I.12	subscr_email_cause	X	X					
33	I.13	bani_campanii	X	X					
34	I.14	date_personale_conc	X	X					
35	I.15	copii_documente	X	X					
36	I.16.1	constr_documente	X						
37	I.16.2	constr_parole		X					
38	I.16.3	constr_confid_info			X				
39	I.17	ajutor_card	X	X					
40	I.18	contacte_necun	X	X					
41	I.19	cont_online_comun	X	X					
42	I.20	msg_castig	X	X					
43	I.21.1	msg_castig_react 1	X						
44	I.21.2	msg_castig_react 2		X					
45	I.21.3	msg_castig_react 3			X				
46	I.21.4	msg_castig_react 4				X			
47	I.22	Victima	X	X					
48	I.23.1	furt_date_pers	X						
49	I.23.2	furt_ID		X					
50	I.23.3	Virusare			X				
51	I.23.4	victima_altele				X			
52	I.24	victime_cunostinte	X	X					
53	I.25	descr_reac_victima	X						
54	I.26.1	RO_preg_atac	X	X					
55	I.26.2	RO_preg_motiv	X						
56	I.27.1	imp_curs_sec_info_pre-univ	X	X	X	X	X		
57	I.27.2	imp_curs_sec_info_univ	X	X	X	X	X		
58	I.27.3	imp_curs_sec_info_motiv	X						

ANEXA NR.3.
Organigrama domeniilor guvernanței securității cibernetice



Această carte reprezintă publicarea tezei de doctorat „*GUVERNANȚA SECURITĂȚII NAȚIONALE: MANAGEMENTUL SECURITĂȚII SPAȚIULUI VIRTUAL ÎNTRE REALISM ȘI SUPRANAȚIONALISM*”, prin Editura PRESA UNIVERSITARĂ CLUJEANĂ cu sprijinul financiar din partea FUNDAȚIEI ȘINCA.

Teza reprezintă rezultatul obținut în urma a șapte ani de intensă documentare și cercetare în Europa, Statele Unite ale Americii și Republica Populară Chineză.

Mulțumesc întregii mele familii pentru încrederea și susținerea acordată în toți acești ani, dar în mod special soției mele Tatiana și copiilor mei David și Victoria, din ale căror resurse și prețios timp am răpit, pentru a finaliza studiile doctorale!

Summa cum Laude este în schimb al lui Dumnezeu!

„Fiat Sancta Sapientia”

UNIVERSITAS CLAUDIOPOLITANA
ROMANIA
PRESA UNIVERSITARĂ

ISBN: 978-606-37-2251-6